HOÀNG CHÚNG

SỐ HỌC

BÀ CHÚA CỦA TOÁN HỌC

NHÀ XUẤT BẢN GIÁO DỤC

Hoàng Chúng

SỐ HỌC

Bà Chúa Của Toán Học

(Xuất bản lần thứ năm)

NHÀ XUẤT BẢN GIÁO DỤC 1997

LỜI NÓI ĐẦU

Số học, ngành lâu đời nhất và đầy hấp dẫn của toán học, đã từng được một nhà toán học nổi tiếng gọi là " bà chúa của toán học ". Các bài toán số học đã làm say mê nhiều người, từ những nhà toán học lỗi lạc của mọi thời đại đến đông đảo các bạn yêu toán. Thế giới các con số, rất quen thuộc với chúng ta trong cuộc sống hàng ngày, là một thế giới hết sức kì lạ, đầy bí ẩn : loài người đã phát hiện trong đó biết bao tính chất rất hay, nhiều quy luật rất đẹp và có khi rất bất ngờ, đồng thời cũng đang chịu bó tay trước nhiều sự kiện, nhiều dự đoán. Điều lí thú là nhiều mệnh đề khó nhất của số học được phát biểu rất đơn giản, ai cũng hiểu được; nhiều bài toán khó có thể giải rất sáng tạo với những kiến thức số học phổ thông. Không ở đâu như trong số học, chúng ta lại có thể lần theo được dấu vết của những bài toán cổ xưa để đến được với những vấn đề mới đang chờ người giải.

Chính vì các lẽ trên đây mà môn số học tuy chỉ được học ở 6 – 7 năm đầu của trường phổ thông, nhưng các bài toán số học luôn có mặt trong các đề thi chọn học sinh giỏi toán ở tất cả các cấp học và ở hầu hết các nước trên thế giới.

Cuốn sách này trình bày một số vấn đề cơ bản của số học phù hợp với trình độ học sinh khá giỏi toán cấp 2 và 3. Sách gồm có 4 chương và một phụ lục; sau mỗi chương (hoặc phần của chương) có nhiều bài tập từ dễ đến tương đối khó. Các chương độc lập với nhau, bạn có thể đọc chương nào trước cũng được (bỏ qua các chỗ in chữ nhỏ). Phần "Gợi ý giải bài tập" chỉ giúp bạn khi gặp khó khăn, và tác giả luôn hi vọng rằng bạn đọc sẽ có những ý hay hơn , sáng tạo hơn. So với bản in lần thứ nhất (1991), bản in lần thứ hai này có một số sửa chữa nhỏ, đặc biệt là bỏ đi Phụ lục 2 (Hoán vị và tổ hợp, công thức Newton) vì nội dung này đã được trình bày đầy đủ trong sách giáo khoa Giải tích 12, kể từ năm học 1992-93.

Tác giả xin chân thành cám ơn những nhận xét quý báu của bạn đọc.

Thành phố Hồ Chí Minh, tháng 6 năm 1993

HOÀNG CHÚNG

CÁC KÝ HIỆU :

∇	Mở đầu phép chứng minh một định lí, lời giải một bài toán
□	Kết thúc chứng minh một định lí, lời giải một bài toán

Các số nói đến trong sách này, nếu không ghi chú gì khác, đều là số nguyên (thuộc **Z**). Riêng trong chương 2 và chương 4 chỉ xét các số tự nhiên (thuộc **N**).

Trong LẦN XUẤT BẢN THỨ NĂM
trang 88 được viết lại cho phù hợp với thành tựu mới ;
một số sai sót do chế bản in đã được sửa.

CHƯƠNG 1

PHÉP CHIA CÓ DƯ. ĐỒNG DƯ THỨC VÀ PHƯƠNG TRÌNH ĐỒNG DƯ

Từ Hàn Tín đến Gauss

Trong một cuốn sách toán của Trung Quốc cách đây khoảng 1500 năm, có giải một bài toán gọi là *Hàn Tín điểm binh* như sau :

Bảo lính sắp hàng 3, hàng 5 rồi hàng 7, mỗi lần sắp thì đếm số lẻ ở hàng cuối cùng. Nhân số lẻ hàng 3 cho 70, số lẻ hàng 5 cho 21, số lẻ hàng 7 cho 15 rồi cộng lại. Lấy số thành thêm một bội của 105 thì được số lính.

Thí dụ: nếu sắp hàng 3 lẻ 2,hàng 5 lẻ 3, hàng 7 lẻ 4 thì số lính là

$$x = 2.70 + 3.21 + 4.15 + k.105 = 263 + k.105.$$

Nếu biết chừng số lính từ 800 đến 900 thì có $x = 893$ (lấy $k = 6$).

"Qui tắc điểm binh" trên đây được tóm tắt cho dễ nhớ trong bốn câu thơ.

Đến thế kỉ thứ 13, nhà toán học Trung Quốc Tần Cửu Thiều đã trình bày đầy đủ hơn phương pháp giải những bài toán tương tự bài toán Hàn Tín điểm binh, thí dụ bài toán *Mất trộm gạo* sau đây:

Có một nhà mất trộm gạo. Nhà đó có ba thùng gạo đầy và bằng nhau, nhưng không biết là bao nhiêu. Sau khi mất thì thấy thùng bên trái còn một hộc, thùng giữa còn 1 thăng 4 hộc, thùng bên phải còn một hộc. Về sau bắt được ba tên trộm Giáp, At, Bính. Giáp khai rằng ban đêm sờ được cái gáo cho vào đong gạo thùng bên trái đổ vào túi, At khai rằng đá phải chiếc giầy gỗ cho vào thùng giữa đong gạo, Bính khai rằng sờ được cái bát son cho vào thùng bên phải đong gạo; lấy về ăn lâu ngày, quên mất không biết là bao nhiêu. Tìm tang vật thì thấy: gáo đựng 1 thăng 9 hộc, giầy gỗ đựng 1 thăng 7 hộc, bát son 1 thăng 2 hộc. Theo tang vật, tìm xem mỗi tên lấy trộm bao nhiêu ? (1 thăng bằng 10 hộc)

Để giải bài toán *Hàn Tín điểm binh* ta phải tìm x sao cho

x chia cho 3, dư 2		x – 2 chia hết cho 3
x chia cho 5, dư 3	hay là	x – 3 chia hết cho 5
x chia cho 7, dư 4		x – 4 chia hết cho 7

Tương tự như vậy với bài toán *Mất trộm gạo.* Với phương pháp giải các bài toán này, các nhà toán học Trung Quốc thời ấy đã biết sử dụng các định lí về chia hết, sớm có khái niệm về đồng dư thức, về giải phương trình đồng dư mà mãi đến đầu thế kỉ thứ 19, nhà toán học Đức lỗi lạc *C.F.Gauss* (Gau-xơ, 1777-1855) mới xây dựng thành một lí thuyết tương đối hoàn chỉnh.

■ 1 - Phép chia hết và phép chia có dư

1-1-Cho hai số nguyên a và b (b > 0). Chia a cho b, ta có: a chia hết cho b hoặc a không chia hết cho b.

1) *a chia hết cho b* hay *a là bội của b*, được kí hiệu là a ⋮ b. Ta cũng nói: *b chia hết a*, hay *b là ước của a* và kí hiệu là

$b|a$.

$a \vdots b$ (hay $b|a$) khi và chỉ khi có số nguyên q sao cho $a = bq$.

$$a \vdots b \Leftrightarrow a = bq.$$

Thí dụ : $18 = 3.6 \Leftrightarrow 18 \vdots 3$ hay $3|18$.

2) *a không chia hết cho b*.Trong trường hợp này, khi chia cho b, ta được thương gần đúng là q và số dư là r ($0 < r < b$) Ta viết được:

$$a = bq + r \text{ với } 0 < r < b$$

Thí dụ:- Với $a = 19$, $b = 3$ ta có $19 = 3.6 + 1$.

Chia 19 cho 3 được thương gần đúng là 6 và số dư là 1.

- Với $a = -25$, $b = 7$, ta có $-25 = 7.(-4) + 3$.

Chia -25 cho 7 được thương gần đúng là -4 và dư là 3.

- Với $a = 5$, $b = 11$, ta có $5 = 11.0 + 5$.

Chia 5 cho 11 được thương gần đúng là 0 và số dư là 5.

Một cách tổng quát, có thể nói rằng:

Khi chia một số nguyên a cho một số nguyên $b > 0$, ta luôn có một số dư duy nhất là r với $0 \leq r < b$ (a chia hết cho b nếu $r = 0$, a không chia hết cho b nếu $r \neq 0$). Số dư r luôn nhỏ hơn b, tức là lớn nhất chỉ bằng $b - 1$.

Khi chia một số nguyên a cho một số nguyên b>0 thì số dư là một trong b số từ 0 đến b – 1.

Thí dụ:- Chia một số cho 2 thì số dư là một trong hai số: 0 hoặc 1.

- Chia một số cho 3 thì số dư là một trong ba số: 0,1 hoặc 2.

- Chia một số cho 5 thì số dư là một trong năm số: 0,1,2,3 hoặc 4.

1.2 - Trong trường hợp *a không chia hết cho b* (số dư $r \neq 0$), thay vì lấy $r > 0$ (từ 1 đến $b - 1$), để tiện lợi trong chứng minh và giải toán, nhiều khi người ta cũng lấy số dư là số âm r' với $r' = r - b$ (do đó $|r'| < b$).

Thí dụ:- Chia 23 cho 3, được số dư là 2:

$$23 = 3.7 + 2.$$

Ta gọi 7 là *thương gần đúng thiếu*, vì $3.7 = 21 < 23$.

Cũng có thể viết:

$$23 = 3.8 + (-1).$$

Ta gọi 8 là *thương gần đúng thừa*, vì $3.8 = 24 > 23$, và số dư là -1.

- Chia 52 cho 6, lấy thương gần đúng thiếu là 8, ta có số dư là 4:

$$52 = 6.8 + 4 .$$

Nếu lấy thương gần đúng thừa là 9 thì có số dư là $4 - 6 = -2$:

$$52 = 6.9 + (-2).$$

- Chia -36 cho 5, ta viết được:

$$-36 = 5.(-8) + 4$$

hoặc là

$$-36 = 5.(-7) + (-1).$$

Số -8 là thương gần đúng thiếu, vì $5.(-8) = -40 < -36$, và ta có số dư là 4. Số -7 là thương gần đúng thừa, vì $5.(-7) = -35 > -36$, và ta có số dư là -1.

Coi số dư có thể là số âm như trên, ta có:

- Khi chia một số cho 2 thì số dư là 0 hoặc 1, do đó mọi số nguyên đều có dạng $2k$ (bội của 2, số chẵn) hoặc $2k + 1$ (số lẻ), trong đó k là một số nguyên.

Nếu số dư trong phép chia cho 2 là 1 thì có thể coi số dư là $1 - 2 = -1$, do đó có thể nói: mọi số nguyên đều có dạng $2k$ hoặc $2k - 1$.

- Khi chia một số nguyên cho 3 thì số dư là 0,1 hoặc 2, do đó mọi số nguyên đều có dạng 3k (bội của 3) hoặc 3k + 1 (bội của 3 cộng 1) hoặc 3k + 2 (bội của 3 cộng 2). Với số dư là 2 thì có thể coi số dư là −1, vì vậy có thể nói mọi số nguyên đều có dạng 3k hoặc 3k±1.

Tương tự như vậy, nếu xét phép chia cho 4 thì ta có: mọi số nguyên đều có dạng 4k, 4k ± 1 hoặc 4k + 2 (hay là 4k, 4k ± 1 hoặc 4k − 2); nếu xét phép chia cho 5 thì có: mọi số nguyên đều có dạng 5k, 5k ± 1 hoặc 5k ± 2;v.v...

Ta có kết quả tổng quát như sau:

$$a = bq + r \ (b > 0)$$

r là số dư khi chia a cho b> 0:

b chẵn $\Rightarrow r = 0, \pm 1, \pm 2, .., +\frac{b}{2}$

(hoặc $r = 0, \pm 1, \pm 2, .., -\frac{b}{2}$)

b lẻ $\Rightarrow r = 0, \ \pm 1, \pm 2, .., \pm\frac{b-1}{2}$

1.3 - Ước chung lớn nhất và bội chung nhỏ nhất

Cho hai số nguyên dương a và b. *Ước chung lớn nhất của a và b* được kí hiệu là ƯCLN (a,b) hay là (a,b).Một số d là ước chung của a và b khi và chỉ khi d là ước của ƯCLN (a,b):

$$d | a \text{ và } d | b \Leftrightarrow d | (a,b).$$

Bội chung nhỏ nhất của a và b được kí hiệu là BCNN (a,b) hay là [a,b]. Một số m là bội chung của a và b khi và chỉ khi m là bội của BCNN (a,b) :

$$m \vdots a \text{ và } m \vdots b \Leftrightarrow m \vdots [a,b]$$

Hai số a và b được gọi là *nguyên tố cùng nhau* khi và chỉ khi (a,b) = 1.

Ta đã biết cách tìm (a,b) và [a,b] dựa vào sự phân tích a và b ra thừa số nguyên tố. Thí dụ:

$a = 126 = 2.3^2.7 \qquad b = 735 = 3.5.7^2$

$\Rightarrow (a,b) = 3.7 = 21 \qquad [a,b] = 2.3^2.5.7^2 = 4410$.

Có thể chứng minh được rằng:

$$[a,b] = \frac{ab}{(a,b)}.$$

Từ đó: $[a,b] = ab$ nếu $(a,b) = 1$.

1.4 - Thuật toán Euclide (Ơclit)

Có thể tìm ƯCLN của hai số, dựa vào định lí về phép chia có dư, mà không cần đến việc phân tích các số đã cho thành thừa số nguyên tố.

Cho hai số nguyên dương a,b và giả sử a>b.

Trước hết, ta chú ý rằng nếu b là ước của a thì (a,b) = b. Thí dụ: 80 = 16.5 , do đó (80,16) = 16.

Xét trường hợp b không phải là ước của a. Thí dụ: a = 702, b = 306, và phải tìm (702,306).

Ta chia 702 cho 306, được thương là 2 và số dư là 90 :

$$702 = 306.2 + 90$$

Vận dụng tính chất: nếu một số là ước của mỗi số hạng của một tổng (hiệu) thì nó là ước cuả tổng (hiệu) ấy, ta có: mọi ước chung của 702 và 306 cũng là ước của 702 – 306.2 = 90, do đó cũng là ước chung của 306 và 90. Ngược lại, mọi ước chung của 306 và 90 cũng là ước của 306.2 + 90 = 702, do đó cũng là ước chung của 702 và 306, vì vậy (702,306) = (306,90) và ta đã đưa việc tìm ƯCLN của hai số đã cho về việc tìm ƯCLN

của hai số tương ứng bé hơn. Tiếp tục nhiều lần như vậy, cuối cùng ta đi đến việc tìm ƯCLN của hai số mà số này là ước của số kia và có ngay được ƯCLN. Ta viết được:

$$702 = 306.2 + 90 \Rightarrow (702,306) = (306,90)$$

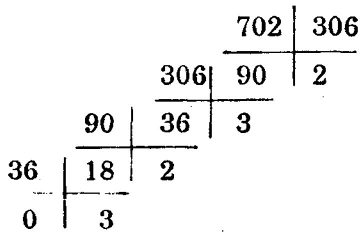
$$306 = 90.3 + 36 \Rightarrow (306,90) = (90,36)$$

$$90 = 36.2 + 18 \Rightarrow (90,36) = (36,18)$$

$$36 = 18.2 \Rightarrow (36,18) = 18$$

Vậy $(720,306) = 18$

Trong thực hành,người ta đặt phép tính như sau:



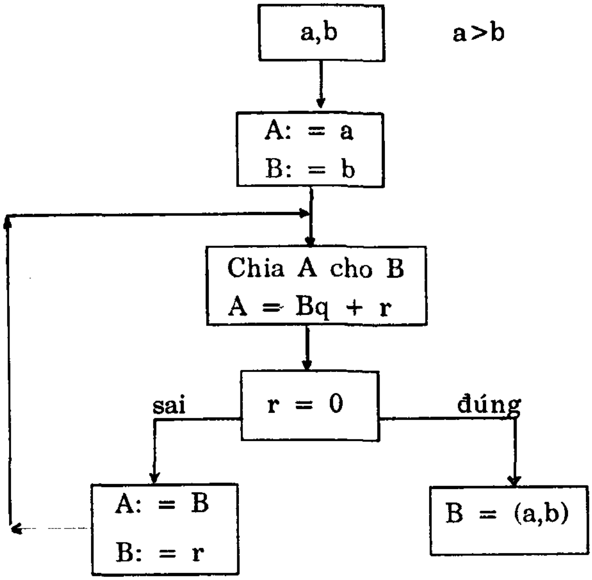
Việc thực hiện một dãy phép chia liên tiếp như trên để tìm ƯCLN của hai số được gọi là *thuật toán Euclide.* Như đã thấy qua thí dụ ở trên, thuật toán Euclide dựa vào hai mệnh đề sau đây:

1) $a = bq \Rightarrow (a,b) = b$

2) $a = bq + r\ (r \neq 0) \Rightarrow (a,b) = (b,r)$

Có thể lặp lại các lập luận trong thí dụ đã xét (với $a = 702$, $b = 306$) để chứng minh mệnh đề 2.

Thuật toán Euclide có thể mô tả bằng một sơ đồ như sau (trong đó A: = a có nghĩa là A lấy giá trị a)



Nếu thực hiện thuật toán Euclide để tìm ƯCLN của hai số, mà đến lúc nào đó ta có số dư là 1 thì hai số đã cho là nguyên tố cùng nhau. Thí dụ: tìm (87,25), ta có:

$87 = 25.3 + 12 \Rightarrow (87,25) = (25,12)$

$25 = 12.2 + 1 \Rightarrow (25,12) = (12,1)$

Vậy $(87,25) = (12,1) = 1$

Áp dụng- Giải bài toán sau:

Cho n là một số tự nhiên bất kì. Hãy chứng minh phân thức $\frac{21n+4}{14n+3}$ *không thể giản ước được.*

(Đề thi học sinh giỏi toán cấp II toàn quốc, 1970). Ta áp dụng thuật toán Euclide để tìm ƯCLN của hai số 21n +4 và 14n +3:

$21n + 4 = (14n + 3).1 + 7n + 1 \Rightarrow (24n + 4, 14n + 3)$
$= (14n + 3, 7n + 1)$

$14n + 3 = (7n + 1).2 + 1 \Rightarrow (14n + 3, 7n + 1) = (7n + 1, 1)$

Vậy $(21n + 4, 14n + 3) = (7n + 1, 1) = 1$.

Hai số $21n + 4$ và $14n + 3$ có ƯCLN là 1, nên phân thức $\dfrac{21 + 4}{14n + 3}$ không thể giản ước được.

Sau đây là một số định lí quan trọng, thường được dùng khi giải các bài toán về chia hết:

Định lí 1

a) $(ca,cb) = c(a,b)$

b) $\left(\dfrac{a}{c},\dfrac{b}{c}\right) = \dfrac{(a,b)}{c}$ với c là ước chung của a và b.

∇ a) Dùng thuật toán Euclide để tìm (a,b), ta được (a,b) = d. Sau đó , ta nhân cả hai vế của tất cả các đẳng thức trong khi thực hiện thuật toán đó với số c. Như vậy, a,b và tất cả các số dư đều được nhân với c, do đó $(ca,cb) = cd = c(a,b)$. □

∇ b) $(a,b) = \left(c\dfrac{a}{c}, c\dfrac{b}{c}\right) = c\left(\dfrac{a}{c}, \dfrac{b}{c}\right)$ □

Định lí 2 *Nếu tích a.c chia hết cho b và a,b nguyên tố cùng nhau thì c chia hết cho b :*

$$a.c \vdots b \text{ và } (a,b) = 1 \Rightarrow c \vdots b .$$

∇ $a.c \vdots b$ và $bc \vdots b \Rightarrow$ b là ước chung của ac và bc.

$(a,b) = 1 \Rightarrow (ac,bc) = c \Rightarrow$ c là bội của b. □

Định lí 3 *Nếu c chia hết cho a và cho b mà a,b nguyên tố cùng nhau thì c chia hết cho tích a.b .*

∇ $c \vdots a \Rightarrow c = ac_1$

$c \vdots b \Rightarrow c = ac_1 \vdots b$, mà $(a,b) = 1 \Rightarrow c_1 \vdots b$

$\Rightarrow c_1 = bc_2 \Rightarrow c = abc_2 \Rightarrow c \vdots ab$ □

1.5- Định lí về phép chia có dư

Trên đây, chúng ta đã thường xuyên sử dụng định lí về phép chia có dư. Sau đây là chứng minh của định lí trong trường hợp a và b đều là số tự nhiên .

Định lí: Với mọi $a,b \in \mathbb{N}$ $(b \neq 0)$ *bao giờ cũng có duy nhất cặp số* $q,r \in \mathbb{N}$ *thỏa mãn:*

(1) $a = bq + r$, với $0 \le r < b$.

Nếu $a < b$ thì $q = 0$, $r = a$ thỏa mãn (1) .

Nếu $a = b$ thì $q = 1$, $r = 0$ thỏa mãn (1) .

Nếu $a > b$, ta viết dãy các hiệu số sau đây:

$$a,\ a-b,\ a-b.2,\ a-b.3,\dots$$

cho đến khi có số âm đầu tiên thì dừng lại. Gọi số không âm nhỏ nhất trong dãy trên là $a-bq$ (≥ 0) thì số âm đầu tiên là $a-b(q+1)$. Đặt $a-bq = r$ (≥ 0) hay $a = bq + r$ thì $r < b$ (vì $a-b(q+1) = (a-bq)-b = r-b < 0$), tức là $0 \le r < b$.

Như vậy, trong mọi trường hợp, ta đều có cặp số $q,r \in \mathbb{N}$ thỏa mãn (1).

Ta chứng minh tiếp rằng cặp số q,r thỏa mãn (1) là duy nhất. Thật vậy, giả sử có hai cặp q_1,r_1 và q,r như vậy, nghĩa là:

$a = bq_1 + r_1$, $0 \le r_1 < b$

$a = bq + r$, $0 \le r < b$.

Không mất tính tổng quát, có thể giả sử $r \ge r_1$. Từ hai đẳng thức trên,suy ra

$$b(q_1 - q) = r - r_1 .$$

Rõ ràng là $r - r_1 < b$,

tức là $b(q_1 - q) < b$.

Trong tập hợp số tự nhiên, bất đẳng thức này xảy ra khi và chỉ khi $q_1 - q = 0$, tức $q_1 = q$, điều này kéo theo $r_1 = r$. Như vậy cặp số q,r thỏa mãn (1) là duy nhất.

1.6- Các bài toán về chia hết và phương hướng tìm lời giải

Các bài toán về chia hết có nhiều dạng; sau đây là một số hướng tìm lời giải, có thể giúp ích trong nhiều trường hợp.

Cho một biểu thức A (n), phụ thuộc số n ($n \in Z$ hay $n \in Z'$,một tập con của Z).

a) Để chứng minh A (n) chia hết cho một số nguyên tố p, có thể xét mọi trường hợp về số dư khi chia n cho p (0, $\pm 1, \ldots, \pm \frac{p-1}{2}$*)* .

Thí dụ 1- Chứng minh rằng

$$A(n) = n(n^2 + 1)(n^2 + 4) \vdots 5$$

với mọi số nguyên n.

∇ Xét mọi trường hợp:

+ n chia hết cho 5, rõ ràng $A(n) \vdots 5$.

+ n không chia hết cho 5 thì *n* có dạng

$5k \pm 1$ (chia n cho 5, dư ± 1) hoặc $5k \pm 2$ (dư ± 2).

$n = 5k \pm 1 \Rightarrow n^2 = 25k^2 \pm 10k + 1 \Rightarrow n^2 + 4 \vdots 5.$

$n = 5k \pm 2 \Rightarrow n^2 = 25k^2 \pm 20k + 4 \Rightarrow n^2 + 1 \vdots 5.$

A (*n*) là tích của ba thừa số, trong mọi trường hợp đều có một thừa số chia hết cho 5, vậy $A(n) \vdots 5$ với mọi n. □

b) Để chứng minh A (n) chia hết cho một hợp số m, nói chung nên phân tích m ra thừa số.Giả sử m = p.q.

Nếu p và q là số nguyên tố, hay p và q nguyên tố cùng nhau thì ta tìm cách chứng minh $A(n) \vdots p$ *và* $A(n) \vdots q$ *(từ đó suy ra* $A(n) \vdots pq = m$*).*

Thí dụ 2- Chứng minh rằng tích của ba số nguyên liên tiếp chia hết cho 6.

∇ Gọi ba số nguyên liên tiếp là n, n + 1 và n + 2, tích của chúng là A (n) = n (n + 1) (n + 2). Ta có 6 = 2.3 (2 và 3 là nguyên tố); ta tìm cách chứng minh A (n) ⋮ 2 và A (n) ⋮ 3.

Trong hai số nguyên liên tiếp, n và n + 1, bao giờ cũng có một số chẵn, do đó A (n) ⋮ 2.

Trong ba số nguyên liên tiếp , n , n + 1 và n + 2, bao giờ cũng có một số chia hết cho 3 , vì số dư khi chia n cho 3 chỉ có thể là 0 (n chia hết cho 3) hoặc là 1 (lúc đó n + 2 chia hết cho 3) hoặc là 2 (lúc đó n + 1 chia hết cho 3), do đó n (n + 1) (n + 2) ⋮ 3.

A (n) ⋮ 2 và A (n) ⋮ 3, vậy A(n) ⋮ 6. □

Nếu p và q không nguyên tố cùng nhau thì ta phân tích A (n) ra thừa số, chẳng hạn A (n) = B(n).C(n) và tìm cách chứng minh B(n) ⋮ p và C(n) ⋮ q (suy ra A(n) = B(n).C(n) ⋮ p.q = m).

Thí dụ 3- Chứng minh rằng tích của hai số chẵn liên tiếp chia hết cho 8.

∇ Gọi số chẵn đầu tiên là 2n, số chẵn tiếp theo là 2n + 2, tích của chúng là A(n) = 2n (2n + 2).

Ta có 8 = 4.2, và A(n) có thể viết thành A(n) = 4.n(n +1), đây là tích của hai thừa số: một thừa số là 4, chia hết cho 4, và một thừa số là n(n +1) luôn chia hết cho 2.

Vì vậy A(n) = 4.n(n +1) ⋮ 4.2 = 8. □

c) Để chứng minh A(n) chia hết cho m, có thể biến đổi A(n) thành tổng của nhiều số hạng và chứng minh mỗi số hạng chia hết cho m.

Thí dụ 4- Chứng minh rằng lập phương của một số nguyên n bất kì (n > 1) trừ đi 13 lần số nguyên đó thì luôn chia hết cho 6.

(Đề thi học sinh giỏi toán cấp II toàn quốc , 1970)

∇ Phải chứng minh $A(n) = n^3 - 13n \vdots 6$.

Chú ý rằng $13n = 12n + n$ mà $12n \vdots 6$, ta biến đổi A(n) thành $A(n) = (n^3 - n) - 12n$, và tìm cách chứng minh $n^3 - n \vdots 6$. Ta có

$$n^3 - n = n(n^2 - 1) = n(n-1)(n+1)$$

và đây là tích của ba số nguyên liên tiếp: $n-1$, n và $n+1$, tích này chia hết cho 6 (xem thí dụ 2).

A(n) là hiệu của hai số hạng: $n^3 - n$ và $12n$, mỗi số hạng chia hết cho 6, nên $A(n) \vdots 6$. □

d) Để chứng minh một tổng không chia hết cho m, có thể chứng minh một số hạng nào đó không chia hết cho m còn tất cả các số hạng khác đều chia hết cho m.

Thí dụ 5- Chứng minh rằng với mọi số n lẻ:

$n^2 + 4n + 5$ không chia hết cho 8.

∇ Đặt $n = 2k + 1$ (n lẻ) ta có

$$n^2 + 4n + 5 = (2k+1)^2 + 4(2k+1) + 5$$
$$= (4k^2 + 4k + 1) + (8k + 4) + 5$$
$$= (4k^2 + 4k) + (8k + 8) + 2$$
$$= 4k(k+1) + 8(k+1) + 2 .$$

Đây là tổng của ba số hạng, số hạng đầu $4k(k+1)$ chia hết cho 8 (xem thí dụ 3) , số hạng thứ hai $8(k+1)$ cũng chia hết cho 8, riêng số hạng thứ ba là 2 thì không chia hết cho 8, vậy tổng không chia hết cho 8. □

e) Thường phải sử dụng kết quả sau đây:

Nếu số dư khi chia a cho b > 0 là r ($0 < r < b$) *thì số dư khi chia a^n ($n > 1$) cho b là số dư khi chia r^n cho b (số dư này bằng r^n nếu $r^n < b$).*

Thí dụ 6- Trở lại thí dụ 1:

$n(n^2 + 1)(n^2 + 4)$ chia hết cho 5 với mọi n.

Ta có thể trình bày lời giải như sau:

+ n chia cho 5 dư 0 $\Rightarrow n \vdots 5$

+ n chia cho 5 dư ±1

$\Rightarrow n^2$ chia cho 5 dư $(\pm 1)^2 = 1$ $\Rightarrow n^2 + 4 \vdots 5$

+ n chia cho 5 dư ± 2

$\Rightarrow n^2$ chia cho 5 dư $(\pm 2)^2 = 4$ $\Rightarrow n^2 + 1 \vdots 5$

Thí dụ 7- Chứng minh rằng nếu n không chia hết cho 7 thì $n^3 + 1$ hoặc $n^3 - 1$ chia hết cho 7.

∇ n không chia hết cho 7 thì n có dạng

$7k\pm1$, $7k\pm2$ hoặc $7k\pm3$.

$n = 7k\pm 1 \Rightarrow n^3 = 7p\pm 1$

$n = 7k \pm 2 \Rightarrow n^3 = 7q \pm 8 = 7(q \pm1) \pm1$

$n = 7k \pm 3 \Rightarrow n^3 = 7r \pm 27 = 7(r\pm4) \pm1$

Trong mọi trường hợp, $n^3 + 1$ hoặc $n^3 - 1$ là bội của 7.□

g) Có thể dùng các công thức sau đây (dễ dàng kiểm tra lại): Ta đã biết:

$$a^2 - b^2 = (a - b)(a + b)$$

$$a^3 - b^3 = (a - b)(a^2 + ab + b^2)$$

$$a^3 + b^3 = (a + b)(a^2 - ab + b^2)$$

Một cách tổng quát:

(1) $a^n - b^n = (a - b).M$ với n bất kì ,

trong đó $M = a^{n-1} + a^{n-2}b + ... + ab^{n-2} + b^{n-1}$.

(2) $a^n - b^n = (a + b).N$ với n chẵn ,

trong đó $N = a^{n-1} - a^{n-2}b + ... + ab^{n-2} - b^{n-1}$

(3) $a^n + b^n = (a + b).P$ với n lẻ,

trong đó $P = a^{n-1} - a^{n-2}b + \dots - ab^{n-2} + b^{n-1}$

Do đó, theo (1) và (2):

$a^n - b^n$ chia hết cho $a - b$ (nếu $a \neq b$) với n bất kì

$a^n - b^n$ chia hết cho $a + b$ (nếu $a \neq -b$) với n chẵn

Theo (3):

$a^n + b^n$ chia hết cho $a + b$ (nếu $a \neq -b$) với n lẻ.

Thí dụ 8- Chứng minh rằng $2^{4n} - 1 \vdots 15$.

Ta có

$2^4 = 16$, do đó $2^{4n} - 1 = 16^n - 1 = (16 - 1).M = 15.M$.

Thí dụ 9- Chứng minh rằng $2^5 + 3^5 + 5^5 \vdots 5$.

Vì 5 là số lẻ nên $2^5 + 3^5 = (2 + 3).P$

từ đó dễ dàng suy ra điều phải chứng minh.

h) Có thể chứng minh bằng qui nạp toán học.

Thí dụ 10- Chứng minh rằng $16^n - 15n - 1 \vdots 225$.

∇ Với $n = 1$ thì $16^n - 15n - 1 = 16 - 15 - 1 = 0 \vdots 225$.

Giả sử $16^k - 15k - 1 \vdots 225$

ta chứng minh $16^{k+1} - 15(k+1) - 1 \vdots 225$.

Thực vậy:

$16^{k+1} - 15(k+1) - 1 = 16.16^k - 15k - 15 - 1$

$= (16^k - 15k - 1) + 15.16^k - 15$.

Theo giả thiết quy nạp, $16^k - 15k - 1 \vdots 225$

còn $15.16^k - 15 = 15(16^k - 1) \vdots 15.15$ (do $16^k - 1 = (16 - 1).M = 15.M$). Vì vậy

$16^{k+1} - 15(k + 1) - 1 \vdots 225$. □

Bài tập

1.1 - Chứng minh rằng:

a) $89^{26} - 45^{21} \vdots 2$; $1991^{1990} - 1990^{1991}$ không chia hết cho 2;

b) $10^n - 4 \vdots 3$; $9.10^n + 18 \vdots 27$;

c) $41^{10} - 1 \vdots 10$; $9^{2n} - 14 \vdots 5$.

1.2 - a) Chứng minh rằng:

- tích của hai số tự nhiên liên tiếp chia hết cho 2;
- tích của 3 số tự nhiên liên tiếp chia hết cho 6;
- tích của 4 số tự nhiên liên tiếp chia hết cho 24;

b) Tích của 5 số tự nhiên liên tiếp chia hết cho bao nhiêu?

c) Chứng minh rằng tích của hai số chẵn liên tiếp chia hết cho 8.

d) Tích của 3 số chẵn liên tiếp chia hết cho bao nhiêu?

1.3- Chứng minh rằng tích của một số chính phương với số tự nhiên đứng liền trước nó chia hết cho 12 (số chính phương là số bằng bình phương của một số nguyên).

1.4- Cho $A(n) = n(n^2 + 1)(n^2 + 4)$. Tìm điều kiện của n để $A(n) \vdots 120$.

1.5- Chứng minh rằng $(n - 1)(n + 1) n^2 (n^2 + 1) \vdots 60$ với mọi n.

1.6- Chứng minh rằng với mọi n lẻ:

a) $n^2 + 4n + 3 \vdots 8$;

b) $n^3 + 3n^2 - n - 3 \vdots 48$.

1.7- Chứng minh rằng với mọi $n \in \mathbb{N}$:

a) $4^n + 15n - 1 \vdots 9$;

b) $10^n + 18n - 28 \vdots 27$.

1.8- Tìm số dư trong phép chia:

a) bình phương của một số lẻ cho 8 ;

b) 2^{1000} cho 5 ; c) 2^{1000} cho 25.

1.9- Chứng minh rằng

$n^4 + 6n^3 + 11n^2 + 6n$ chia hết cho 24 với mọi $n \in \mathbb{N}$.

(Đề thi học sinh giỏi toán cấp II toàn quốc , 1975)

1.10- Chứng minh rằng một số có dạng $n^4 - 4n^3 - 4n^2 - 16n$ (n là số chẵn >4) thì chia hết cho 384.

(Đề thi học sinh giỏi toán cấp II toàn quốc, 1970)

1.11- Chứng minh rằng với mọi $n \in Z$:

a) $n^2 - n \vdots 2$; b) $n^3 - n \vdots 3$; c) $n^5 - n \vdots 5$.

1.12- Chứng minh rằng:

a) $n^4 - 1 \vdots 8$ với mọi n không chia hết cho 2.

b) $n^6 - 1 \vdots 9$ với mọi n không chia hết cho 3.

1.13- Chứng minh rằng nếu $(n , 6) = 1$ và $n \geq 5$ thì $n^2 - 1 \vdots 24$.

1.14- Chứng minh rằng $3^{6n} - 2^{6n} \vdots 35$ với mọi $n \in \mathbb{N}$.

1.15- Chứng minh rằng:

a) $(a^2 + b^2)(a^2 - b^2) \vdots 15$

b) $ab\,(a^2 + b^2)(a^2 - b^2) \vdots 30$

1.16- Chứng minh rằng:

a) Nếu $m^2 + n^2 \vdots 3$ thì m và $n \vdots 3$;

b) Nếu $m^2 + n^2 \vdots 7$ thì m và $n \vdots 7$;

c) Nếu $m^2 + n^2 \vdots 5$ thì $2m + n \vdots 5$ và $2n - m \vdots 5$

hoặc $2m - n \vdots 5$ và $2n + m \vdots 5$;

d) $m^3 + n^3 \vdots 6$ khi và chỉ khi $m + n \vdots 6$.

1.17- Chứng minh rằng $4a^2 + 3a + 5 \vdots 6$

khi và chỉ khi a và 6 nguyên tố cùng nhau.

1.18- Chứng minh rằng

$n^8 - n^6 - n^4 + n^2 \vdots 1152$ với mọi n lẻ.

1.19- Chứng minh rằng:

a) Trong 11 số nguyên bất kì, bao giờ cũng có hai số có cùng chữ số tận cùng;

b) Trong m + 1 số nguyên bất kì, bao giờ cũng có hai số mà hiệu chia hết cho m;

c) Trong m số nguyên bất kì, bao giờ cũng có một số chia hết cho m hoặc ít nhất hai số có tổng chia hết cho m;

d) Trong 5 số nguyên tùy ý, bao giờ cũng có 3 số có tổng chia hết cho 3.

1.20- Có hay không có một số có dạng

199119911991...1991000...000

chia hết cho 1990 ?

1.21- a) Tổng các bình phương của 5 số nguyên liên tiếp có thể là số chính phương được không ?

b) Tổng các lũy thừa chẵn của 3 số nguyên liên tiếp có thể là lũy thừa chẵn của một số nguyên không ?

1.22- Chứng minh rằng với mọi số nguyên n:

a) $n^2 + n + 2$ không chia hết cho 3;

b) $n^2 + 11n + 39$ không chia hết cho 49;

c) $n^2 + 3n + 5$ không chia hết cho 121 .

1.23- Một số có hai chữ số chia hết cho 7. Chứng minh rằng hiệu các lập phương của hai chữ số đó chia hết cho 7.

1.24- Cho bốn số nguyên a,b,c,d. Chứng minh rằng

$(b - a)(c - a)(d - a)(d - c)(b - d)(c - b) \vdots 12$

1.25- Chứng minh rằng $(a + b + c)^3 - (a^3 + b^3 + c^3) \vdots 24$

nếu a,b,c cùng chẵn hoặc cùng lẻ.

1.26- Chứng minh rằng

$1^3 + 3^3 + 5^3 + 7^3 \vdots 2^3$

1.27- Chứng minh rằng nếu a và b là hai số lẻ thì

$a^3 - b^3 \vdots 2^n$ khi và chỉ khi $a - b \vdots 2^n$.

1.28- Tìm số dư trong phép chia số

$(P - 1)(Q - 1)$ cho 192

trong đó P và Q là hai số chính phương lẻ.

1.29- Chứng minh rằng

$(3 + 3^3 + 3^5 + ... + 3^{2n-1}) \vdots 30$

1.30- Chứng minh rằng

$12^{2n+1} + 11^{n+2} \vdots 133$

1.31- Tìm n > 0 sao cho :

a) $n^2 + 1$ chia hết cho n + 1.

b) $n^2 + 2n + 6$ chia hết cho n + 4.

1.32- Với giá trị nào của n thì $(n + 5)(n + 6) \vdots 6n$?

1.33- Chứng minh rằng

$1^n + 2^n + 3^n + 4^n \vdots 5$

khi và chỉ khi n không chia hết cho 4.

1.34- Chứng minh rằng nếu k lẻ thì

$1 + 2^k + \ldots + (n-1)^k + n^k \vdots 1 + 2 + \ldots + (n-1) + n$

với mọi $n \in Z$.

1.35- Cho $2^n = 10a + b$.

Chứng minh rằng nếu $n > 3$ thì tích a.b chia hết cho 6. (a,b,n là các số nguyên dương và $b < 10$.)

(Đề thi học sinh giỏi toán cấp II toàn quốc, 1985)

1.36- Cho biết

$a_n = 2^{2n+1} + 2^{n+1} + 1$

$b_n = 2^{2n+1} - 2^{n+1} + 1$

$(n = 0, 1, 2, \ldots)$. Chứng minh rằng với mỗi số tự nhiên n có một và chỉ một trong hai số a_n, b_n chia hết cho 5.

1.37- Tìm tất cả các số tự nhiên n để $2^n - 1$ chia hết cho 7.

Chứng minh rằng với mọi số tự nhiên n thì $2^n + 1$ không chia hết cho 7.

(Đề thi vô địch toán quốc tế, 1964).

1.38- Chứng minh rằng

a) $11^{10} - 1 \vdots 100$;

b) $2222^{5555} + 5555^{2222} \vdots 7$.

1.39- Chứng minh rằng có vô hạn các số có dạng

$a_n = 2^n - 3 \ (n \geq 2)$

đôi một nguyên tố cùng nhau.

1.40- Với giá trị nào của số tự nhiên n thì

a) $3^n + 63 \vdots 72$;

b) $20^n + 16^n - 3^n - 1 \vdots 323$

1.41- Xét dãy số sau đây : 1,1,2,3,5,8,13,21,...

được lập như sau: hai số hạng đầu tiên là 1, sau đó mỗi số hạng tiếp sau thì bằng tổng hai số hạng đứng trước nó. Gọi a_1 là số hạng thứ nhất, a_2 là số hạng thứ hai, a_k là số hạng thứ k, ta có:

$$a_1 = a_2 = 1,\ a_{k+1} = a_k + a_{k-1} \text{ (với mọi } k > 1).$$

Dãy số trên được gọi là dãy số Fibonacci (Phibonaxi, 1180 - 1240, nhà toán học Ý). Chứng minh rằng hai số hạng liên tiếp trong dãy số Fibonacci là nguyên tố cùng nhau:

$$(a_k, a_{k+1}) = 1 \text{ với mọi } k > 1.$$

1.42- Tìm hai số tự nhiên a và b biết:

a) $a + b = 128$ và $(a,b) = 16$;

b) $a.b = 216$ và $(a,b) = 6$;

c) $a.b = 18$ và $[a,b] = 160$;

d) $7a = 11b$ và $(a,b) = 45$.

1.43- Chứng minh rằng:

a) $(a,b) = (a, a \pm b)$

b) $(a,c) = 1$ và $(b,c) = 1 \Rightarrow (ab, c) = 1$.

c) $(a,b) = 1 \Rightarrow (ab, a \pm b) = 1$

d) $(a,b) = 1 \Rightarrow (a+b, a-b) = 1$ hoặc $= 2$.

1.44- Chứng minh rằng

$$\frac{a^3 + 2a}{a^4 + 3a^2 + 1} \text{ là tối giản.}$$

1.45- Tìm n để cho các phân số sau đây là tối giản:

a) $\dfrac{n + 13}{n - 2}$;

b) $\dfrac{18n + 3}{21n + 7}$

c) $\dfrac{5n + 6}{6n + 5}$

1.46- Chứng minh rằng:

a) $(5a + 3b, 13a + 8b) = (a,b)$

b) $(18a + 5b, 11a + 3b) = (a,b)$

1.47- Biết rằng $(a,b) = 1$, hãy tìm $(11a + 2b, 18a + 5b)$.

1.48- Tìm: a) $(n, n + 2)$; b) $(n, n + 1)$.

1.49- Tìm BCNN của ba số tự nhiên liên tiếp.

1.50- Chứng minh rằng:

a) Trong 5 số dương liên tiếp:

- không có hai số nào có ước chung $d \geq 5$;
- có ít ra là một số nguyên tố với bốn số kia.

b) Trong 6 số nguyên dương liên tiếp:

- không có hai số nào có ước chung $d \geq 6$;
- có ít ra là một số nguyên tố với năm số kia.

1.51- Cho $a = 123456789$ và $b = 987654321$.

a) Tìm (a,b)

b) Tìm số dư khi chia [a,b] cho 11.

1.52- Cho $A = m + n$ và $B = m^2 + n^2$, trong đó *m* và *n* là những số tự nhiên nguyên tố cùng nhau. Tìm ước chung lớn nhất của A và B.

(Đề thi học sinh giỏi toán cấp II toàn quốc, 1980)

1.53- Cho hai số tự nhiên a và b. Có thể phân tích a và b ra thừa số nguyên tố như sau:

$$a = p_1^{a_1} . p_2^{a_2} \dots p_k^{a_k}$$

$$b = p_1^{b_1} . p_2^{b_2} \dots p_k^{b_k},$$

trong đó $p_1, p_2, \dots p_k$ là các số nguyên tố, đôi một phân biệt, $a_1, a_2, \dots a_k$ và $b_1, b_2, \dots b_k$ là các số tự nhiên (chú ý rằng $p^0 = 1$).

Thí dụ:

$$a = 24 = 2^3.3 = 2^3.3.5^0$$

$$b = 225 = 3^2.5^2 = 2^0.3^2.5^2.$$

Ta dùng kí hiệu:

min (p,q) là số nhỏ trong hai số p,q

max (p,q) là số lớn trong hai số p,q.

Thí dụ: min (3,8) = 3 còn max (3,8) = 8 .

Với kí hiệu như trên, ta có:

$$(a,b) = p_1^{\min(a_1, b_1)} . p_2^{\min(a_2, b_2)} \dots p_k^{\min(a_k, b_k)}$$

$$[a,b] = p_1^{\max(a_1, b_1)} . p_2^{\max(a_2, b_2)} \dots p_k^{\max(a_k, b_k)}$$

Hãy chứng minh rằng: a) $[a,b] = \frac{ab}{(a,b)}$

b) Với mọi số tự nhiên p,q,r, ta có

$\max(p, \min(q,r)) = \min((\max(p,q), \max(p,r))$.

Từ đó suy ra rằng: $[a, (b,c)] = ([a,b], [a,c])$

2 - ĐỒNG DƯ THỨC

2.1 - Định nghĩa

Cho một số nguyên m >0. Nếu hai số nguyên a và b cho cùng số dư khi chia cho m (tức là a – b chia hết cho m) thì ta nói rằng

a đồng dư với b theo modun m

và viết $a \equiv b \pmod m$

Đây là một *đồng dư thức* (với a là vế trái, b là vế phải).

Thí dụ:

$46 \equiv 16 \pmod{10}$ vì $46 - 16 = 30 \vdots 10$

$5 \equiv 1 \pmod 2$ vì $5 - 1 = 4 \vdots 2$

$2 \equiv 16 \pmod 3$ vì $-2 - 16 = -18 \vdots 3$

Nếu a - b chia hết cho *m* thì có một số nguyên *t* sao cho

$$a - b = m.t$$

Do đó, theo định nghĩa của đồng dư thức:

$$a \equiv b \pmod m$$

có nghĩa là $a - b = m.t$ (t nguyên)

hay $a = b + m.t$

Trong trường hợp $|b| < m$ thì

$$a \equiv b \pmod m$$

có nghĩa là chia a cho m, có dư là b.

Nói riêng: $a \equiv 0 \pmod{m}$

có nghĩa là a chia hết cho m.

Thí dụ :

$12 \equiv 5 \pmod{7}$ nghĩa là: 12 chia cho 7, dư 5;

$17 \equiv -1 \pmod{9}$ nghĩa là: 17 chia cho 9, dư-1;

$35 \equiv 0 \pmod{5}$ nghĩa là: 35 chia hết cho 5.

Nếu $a \equiv b \pmod{m}$ là sai

thì ta cũng viết $a \not\equiv b \pmod{m}$.

Thí dụ: $12 \not\equiv 0 \pmod{10}$, $13 \not\equiv 2 \pmod{4}$.

2.2 - Các tính chất của đồng dư thức

Đồng dư thức có nhiều tính chất *tương tự các tính chất của đẳng thức*. Có thể chứng minh dễ dàng các thính chất sau đây:

a) Ta có

$a \equiv a \pmod{m}$ với mọi a

$a \equiv b \pmod{m} \Rightarrow b \equiv a \pmod{m}$

$a \equiv b \pmod{m}$ và $b \equiv c \pmod{m} \Rightarrow a \equiv c \pmod{m}$

(tính chất thứ ba được gọi là tính chất bắc cầu của quan hệ đồng dư).

Do có các tính chất này, quan hệ đồng dư (theo modun m) chia tập hợp các số nguyên ra thành m lớp; bất cứ số nguyên nào cũng thuộc một trong m lớp đó, hai số trong cùng một lớp thì đồng dư với nhau (theo modun m), hai số khác lớp thì không đồng dư với nhau (theo modun m). Thí dụ: quan hệ đồng dư theo modun 2 chia tập hợp các số nguyên ra thành 2 lớp: lớp các số đồng dư với 0, mod 2(các số chia hết cho 2) và lớp các số đồng dư với 1, mod 2 (các số chia cho 2, còn dư 1) ; - quan hệ đồng dư theo mod 3 chia tập hợp các số nguyên thành 3 lớp:

lớp các số đồng dư với 0, mod 3(các số bội của 3), lớp các số đồng dư với 1, mod 3(bội của 3 cộng 1), lớp các số đồng dư với 2, mod 3(bội của 3 cộng 2); v.v... Đó là cách diễn đạt khác (dùng khái niệm đồng dư) của điều chúng ta đã biết: mọi số nguyên đều có dạng 2k hoặc 2k + 1; mọi số nguyên đều có dạng 3k, 3k + 1 hoặc 3k + 2; v.v... (xem tr.9).

b) Ta có thể *cộng, trừ hay nhân từng vế hai đồng dư thức theo cùng modun.*

Nếu $a \equiv b \pmod{m}$

$c \equiv d \pmod{m}$

thì $a + c \equiv b + d \pmod{m}$

$a - c \equiv b - d \pmod{m}$

$a.c \equiv b.d \pmod{m}$

Từ đó, suy ra rằng: *Có thể cộng hay trừ cùng một số vào hai vế của một đồng dư thức (có thể chuyển một số từ vế này sang vế kia, nhưng phải đổi dấu của nó), có thể nhân hai vế của đồng dư thức với cùng một số, có thể nâng hai vế của đồng dư thức lên cùng một lũy thừa,* nghĩa là

$$a \equiv b \pmod{m} \Rightarrow a \pm c = b \pm c \pmod{m}$$

$$a + c \equiv b \pmod{m} \Rightarrow a \equiv b - c \pmod{m}$$

$$a \equiv b \pmod{m} \Rightarrow n.a \equiv n.b \pmod{m}$$

$$a \equiv b \pmod{m} \Rightarrow a^n \equiv b^n \pmod{m}$$

c) Ta có thể chia hai vế của một đồng dư thức cho ước chung của chúng, nếu ước này nguyên tố với modun m.

∇ Cho $a \equiv b \pmod{m}$ và a,b có ước chung là k, tức là $a = ka'$, $b = kb'$. Thế thì $ka' \equiv kb' \pmod{m}$, nghĩa là $ka' - kb' = k(a' - b')$ chia hết cho m. Nhưng theo giả thiết thì $(k,m) = 1$, nên phải có $a' - b'$ chia hết cho m, tức là $a' \equiv b' \pmod{m}$.□

Thí dụ: Ta có

$$48 \equiv 18 \pmod{10}$$

48 và 18 đều có ước chung là 3, nguyên tố với 10. Có thể chia hai vế cho 3 và được:

$$16 \equiv 6 \pmod{10}$$

Chú ý rằng 48 và 18 cũng có ước chung là 6, nhưng 6 không nguyên tố với 10, ta không thể chia hai vế của đồng dư thức cho 6 được: chia 48 và 18 cho 6 ta có các số tương ứng là 8 và 3, mà $8 \not\equiv 3 \pmod{10}$.

d) Ta có thể nhân hai vế và modun của đồng dư thức với một số nguyên dương.

$a \equiv b \pmod{m} \Rightarrow a.c \equiv b.c \pmod{m.c}$, với $c > 0$

Ta có thể chia hai vế và modun của một đồng dư thức cho ước chung dương của chúng.

Nếu d là ước chung dương của a,b và m thì

$$a \equiv b \pmod{m} \Rightarrow \frac{a}{d} \equiv \frac{b}{d} \left(\bmod \frac{m}{d}\right) \text{ với } d>0.$$

2.3- Một số thí dụ áp dụng

Thí dụ 1- Tìm chữ số sau cùng của các số 6^{713} và 2^{1000}.

∇ Tìm chữ số sau cùng của một số N có nghĩa là tìm số dư của phép chia N cho 10, tức là tìm số không âm nhỏ hơn 10 và đồng dư với N theo modun 10.

Ta có $6^2 = 36 \equiv 6 \pmod{10}$

do đo $\quad 6^n \equiv 6 \pmod{10}$ với mọi $n > 0$.

Suy ra $\quad 6^{713} \equiv 6 \pmod{10}$

tức là chữ số sau cùng của 6^{713} là 6.

Chú ý rằng $2^4 = 16 \equiv 6 \pmod{10}$ và $1000 = 4.250$ ta có:

$$2^{1000} = 2^{4.250} = (2^4)^{250}$$

Do đó $2^{1000} \equiv 6^{250} \equiv 6 \pmod{10}$

tức là chữ số sau cùng của 2^{1000} cũng là 6. ❐

Thí dụ 2- Tìm số dư trong phép chia 3^{100} cho 7.

∇ Ta phải tìm số có giá trị tuyệt đối nhỏ hơn 7,đồng dư với 3^{100} theo mod 7.

Ta có: $3^3 = 27 \equiv -1 \pmod 7$

$$3^{100} = 3^{3.33+1} = (3^3)^{33}.3$$

do đó $(3^3)^3 \equiv (-1)^{33} \pmod 7$ mà $(-1)^{33} = -1$

nên $3^{100} = (3^3)^{33}.3 \equiv -1.3 \pmod 7$

$$3^{100} \equiv -3 \pmod 7$$

Vậy số dư trong phép chia 3^{100} cho 7 là -3 (hay là 4). ❐

Thí dụ 3- Chứng minh một số dấu hiệu chia hết

Cho một số nguyên N. Nếu N có chữ số hàng đơn vị là a, chữ số hàng chục là b, chữ số hàng trăm là c, chữ số hàng nghìn là d,v.v...thì ta có

$$N = a + b.10 + c.10^2 + d.10^3 + \dots$$

Thí dụ:

$$N = 7465 = 5 + 6.10 + 4.10^2 + 7.10^3$$

$$N = 98324 = 4 + 2.10 + 3.10^2 + 8.10^3 + 9.10^4$$

Dấu hiệu chia hết cho 9

Ta có:

$$a \equiv a \pmod 9$$

$$10 \equiv 1 \pmod 9 \Rightarrow b.10 \equiv b \pmod 9$$

$$10^2 \equiv 1 \pmod 9 \Rightarrow c.10^2 \equiv c \pmod 9$$

$$10^3 \equiv 1 \pmod 9 \Rightarrow d.10^3 \equiv d \pmod 9$$

...

Cộng từng vế các đồng dư thức trên, ta được

$N = a + b.10 + c.10^2 + d.10^3 + ... \equiv a + b + c + d + ... \pmod 9$

Như vậy N đồng dư với tổng các chữ số của nó, theo modun 9, do đó *N chia hết cho 9 khi và chỉ khi tổng các chữ số của nó chia hết cho 9.*

Dấu hiệu chia hết cho 11

Ta có: $10 \equiv -1 \pmod{11}$

do đó $10^n \equiv 1 \pmod{11}$ nếu n chẵn

$10^n \equiv -1 \pmod{11}$ nếu n lẻ

Vì vậy

$b.10 \equiv -b \pmod{11}$

$c.10^2 \equiv c \pmod{11}$

$d.10^3 \equiv -d \pmod{11}$v.v...

Do đó

$N = a + b.10 + c.10^2 + d.10^3 + ... = a - b + c - d + ... \pmod{11}$.

Như vậy, *số N chia hết cho 11 khi và chỉ khi tổng $a - b + c - d + ...$ chia hết cho 11.*

Thí dụ:

- Với N = 9526, có $6 - 2 + 5 - 9 = 0 \vdots 11 \Rightarrow 9526 \vdots 11$

- Với N = 37258, có $8 - 5 + 2 - 7 + 3 = 1$ không chia hết cho 11, do đó 37258 không chia hết cho 11.

Bài tập

1.55- Tìm dấu hiệu chia hết cho 4, 8, 25.

1.56- Tìm số dư khi:

a) Chia 8! cho 11 ; b) Chia $1532^5 - 1$ cho 9;

c) Chia 3^{40} cho 83; d) Chia 2^{1000} cho 25;

e) Chia $3012^{93} - 1$ cho 13; g) Chia 4362^{4362} cho 11 ;

h) Chia 35^{150} cho 425;

i) Chia $10^{10} + 10^{10^2} + ... + 10^{10^{10}}$ cho 7.

1.57- Tìm hai chữ số sau cùng của

a) 2^{999} ; b) 3^{999}.

1.58- Chứng minh rằng:

a) $2^{4n} - 1 \vdots 15$; b) $2^{70} + 3^{70} \vdots 13$

c) $20^{15} - 1 \vdots 11.31.61$; d) $1890^{1930} + 1945^{1975} + 1 \vdots 7$;

e) $12^{2n+1} - 11^{n+2} \vdots 133$

1.59- Giải bài 1.38b)

1.60- Giải a) bài 1.23; b) bài 1.37

■ 3 - PHƯƠNG TRÌNH ĐỒNG DƯ

Sau đây chỉ giới thiệu cách giải một số phương trình và hệ phương trình đồng dư bậc nhất một ẩn, thông qua một số thí dụ.

3.1- Phương trình đồng dư bậc nhất (một ẩn)

Tương tự với phương trình bậc nhất trong đại số, phương trình đồng dư bậc nhất (một ẩn) là đồng dư thức có dạng

$$ax \equiv b \pmod{m} \text{ với } a \not\equiv 0 \pmod{m}$$

trong đó a,b và m(m > 0) là các số đã biết và x là ẩn số (số chưa biết, phải tìm).

Thí dụ 1- Giải phương trình đồng dư

$$4x \equiv 5 \pmod{7}$$

Ta phải tìm x sao cho nếu chia 4x cho 7 thì có số dư là 5. Ta biết rằng mọi số nguyên đều đồng dư, theo modun 7, với một trong 6 số: 0,1,2,3,4,5,6 (số dư trong phép chia một số cho 7). Ta cho x lần lượt lấy các giá trị này, rồi tính giá trị của 4x, sau đó tính số dư trong phép chia 4x cho 7;ta có bảng sau đây:

x	0	1	2	3	4	5	6
4x	0	4	8	12	16	20	24
Số dư trong phép chia 4x cho 7	0	4	1	5	2	6	3

Ta thấy rằng với x = 3 thì $4x \equiv 5 \pmod 7$, vậy x = 3 là nghiệm của phương trình đã cho. Rõ ràng là mọi số đồng dư với 3 theo mod 7 cũng là nghiệm của phương trình, nghĩa là phương trình có nghiệm là:

$$x \equiv 3 \pmod 7$$

hay là $x = 3 + 7t$ (t là số nguyên tùy ý).

Ngoài ra, phương trình không có nghiệm nào khác. Người ta nói rằng: Phương trình đồng dư $4x \equiv 5 \pmod 7$ có nghiệm duy nhất là $x \equiv 3 \pmod 7$

(hiểu theo nghĩa: tất cả các nghiệm đều thuộc một lớp các số đồng dư với 3 theo modun 7)

Có thể chứng minh được rằng:

Phương trình đồng dư $ax \equiv b \pmod m$ có nghiệm duy nhất (theo nghĩa vừa nói), nếu a và m nguyên tố cùng nhau.

Cách giải chi tiết như trong thí dụ 1 có thể gợi ý để bạn đọc tìm ra chứng minh của định lí này(xem bài tập 1.63). Trong nhiều trường hợp, có thể thấy ngay được nghiệm qua một vài phép thử.

Thí dụ 2- Giải phương trình đồng dư

$$3x \equiv 2 \pmod{8}$$

Ta có $(3,8) = 1$, phương trình có nghiệm duy nhất. Theo định nghĩa về đồng dư thức, phương trình đã cho tương đương với:

$$3x = 2 + 8t (t \text{ nguyên tùy ý})$$

Dễ thấy rằng có thể lấy $t = -1$ hoặc $t = 2$

Với $t = -1$ thì $3x = 2 - 8 = -6$, do đó $x = -2$

và nghiệm của phương trình đồng dư đã cho là

$$x \equiv -2 \pmod{8}.$$

Nếu lấy $t = 2$ thì có $3x = 2 + 16 = 18$, $x = 6$ và nghiệm là $x \equiv 6 \pmod{8}$.Đây cũng chính là nghiệm đã tìm, vì $6 \equiv -2 \pmod{8}$.

Thí dụ 3- Giải phương trình đồng dư

$$17x \equiv 13 \pmod{11}$$

Các số 17 và 13 lớn hơn 11. Ta chia các số đó cho 11 và được các số dư tương ứng là 6 và 2. Ta có

$17x \equiv 6x \pmod{11}$ và $13 \equiv 2 \pmod{11}$.

Áp dụng tính chất bắc cầu của quan hệ đồng dư, ta được phương trình tương đương với phương trình đã cho:

$$6x \equiv 2 \pmod{11}$$

Có thể chia hai vế cho 2, vì $(2, 11) = 1$

$$3x \equiv 1 \pmod{11}$$

$$3x = 1 + 11t$$

Có thể lấy $t = 1$, $x = 4$ và có nghiệm là $x \equiv 4 \pmod{11}$.

Qua thí dụ 3, thấy rằng bao giờ cũng có thể đưa phương trình đồng dư bậc nhất về dạng $ax \equiv b \pmod{m}$

trong đó $m > a > 0$ và $m > b \geq 0$.

3.2 - Hệ phương trình đồng dư bậc nhất một ẩn

Thí dụ 1- Giải hệ phương trình đồng dư

$$x \equiv 2 \pmod 3 \quad (1)$$

$$x \equiv 3 \pmod 5 \quad (2)$$

Phương trình (1) tương đương với $x = 2 + 3t$ (t nguyên tùy ý). Thay giá trị này của x vào phương trình (2) ta được $2 + 3t \equiv 3 \pmod 5$. Vậy hệ đã cho tương đương với hệ

$$x = 2 + 3t \qquad (1a)$$

$$2 + 3t \equiv 3 \pmod 5 \qquad (2a)$$

Từ phương trình (2a) chuyển 2 từ vế trước ra vế sau và đổi dấu, ta được

$$3t \equiv 1 \pmod 5$$

do đó $$t \equiv 2 \pmod 5$$

hay $$t = 2 + 5k \text{ (k nguyên)}$$

Thay giá trị này của t vào phương trình (1), được

$$x = 2 + 3(2+ 5k) = 8 + 15k$$

hay là $$x \equiv 8 \pmod{15}$$

Đó là nghiệm của hệ phương trình đã cho.

Thí dụ 2- Đối với bài toán *Hàn Tín điểm binh* (xem trang 5), ta phải giải hệ phương trình đồng dư:

$$x \equiv 2 \pmod 3 \qquad (1)$$

$$x \equiv 3 \pmod 5 \qquad (2)$$

$$x \equiv 4 \pmod 7 \qquad (3)$$

Hệ hai phương trình (1), (2) cho ta (xem thí dụ 1):

$$x \equiv 8 \pmod{15}$$

Do đó, hệ ba phương trình đã cho tương đương với hệ:

$$x \equiv 8 \pmod{15}$$

$$x \equiv 4 \pmod 7$$

Hệ này tương đương với

$$x = 8 + 15k \qquad (I)$$

$$8 + 15k \equiv 4 \pmod 7 \qquad (II)$$

Phương trình (II) cho ta

$$15k \equiv -4 \pmod 7$$

hay là $k \equiv 3 \pmod 7$ do đó $k = 3 + 7t$.

Thay giá trị này vào phương trình (I), được

$$x = 8 + 15(3 + 7t) = 53 + 105t \ (t \geq 0).$$

Nếu số lính khoảng 900 thì phải lấy $t = 8$ và được $x = 893$ (người).

Còn về qui tắc: "nhân số lẻ hàng 3 cho 70, số lẻ hàng 5 cho 21, số lẻ hàng 7 cho 15, rồi cộng lại; lấy số thành thêm một bội của 105", xin xem bài tập 1.65.

Bài tập

1.61- Giải phương trình:

a) $5x \equiv 4 \pmod{11}$; b) $7x \equiv 6 \pmod{13}$

c) $(a + b)x \equiv a^2 + b^2 \pmod{ab}$, với $(a,b) = 1$

1.62- Giải phương trình:

a) $6x \equiv 27 \pmod{33}$; b) $(a + 1)x \equiv a^2 - 1 \pmod m$

1.63- Cho $ax \equiv b \pmod m$ với $(a,m) = 1$.

Chứng minh rằng khi x chạy qua m giá trị khác nhau từ 0 đến $m - 1$ thì số dư khi chia ax cho m cũng chạy qua m giá trị đó (chỉ khác về thứ tự mà thôi). (Trong thí dụ 1, giải phương trình đồng dư $4x \equiv 5 \pmod 7$, ta đã cho x chạy qua 7 giá trị từ 0 đến 6, và số dư trong phép chia $4x$ cho 7 cũng chạy qua 7 giá trị đó). Từ đó, suy ra rằng phương trình $ax \equiv b \pmod m$ luôn có nghiệm với $(a,m) = 1$.

1.64- Một lớp gồm 40 học sinh đứng thành vòng tròn và quay mặt vào trong vòng tròn để chơi bóng. Mỗi học sinh nhận được bóng phải ném bóng qua mặt 6 bạn đứng ở tay trái mình. Chứng minh rằng tất cả học sinh trong lớp đều nhận được bóng ném tới mình sau 40 lần ném bóng liên tiếp.

(Đề thi học sinh giỏi toán cấp II toàn quốc, 1987)

1.65- a) Chứng minh rằng hệ phương trình:

$$x \equiv a \pmod p$$
$$x \equiv b \pmod q$$
$$x \equiv c \pmod r$$

(p,q,r là các số nguyên dương đôi một nguyên tố cùng nhau) có nghiệm là:

$$x \equiv Pqr.a + pQr.b + pqR.c \pmod{pqr}$$

trong đó P là số sao cho $Pqr \equiv 1 \pmod p$, Q là số sao cho $pQr \equiv 1 \pmod q$, R là số sao cho $pqR \equiv 1 \pmod r$.

b) Áp dụng: giải bài toán "Hàn Tín điểm binh".

c) Mở rộng qui tắc trên đây để giải hệ phương trình:

$$x \equiv 1 \pmod 3$$
$$x \equiv 4 \pmod 5$$
$$x \equiv 2 \pmod 7$$
$$x \equiv 9 \pmod{11}$$

1.66- Tìm tất cả các số tự nhiên ≤ 1000 mà khi chia cho 3,5,9,11 thì cho số dư lần lượt là 1,3,4,9.

1.67- Giải bài toán "Mất trộm gạo" (tr.6)

1.68- Giải các hệ phương trình :

a) $x \equiv 4 \pmod 5$, $x \equiv 1 \pmod{12}$, $x \equiv 7 \pmod{14}$

b) $5x \equiv 1 \pmod{12}$, $5x \equiv 2 \pmod 8$, $7x \equiv 3 \pmod{11}$

1.69- Giải các hệ phương trình :

a) $x \equiv a \pmod 6$, $x \equiv 1 \pmod 8$

b) $x \equiv 5 \pmod 8$, $x \equiv 8 \pmod{21}$, $x \equiv a \pmod{35}$

1.70- Xác định số nguyên a để các hệ phương trình sau đây có nghiệm:

a) $x \equiv 3 \pmod{11}$, $x \equiv 1 \pmod{15}$, $x \equiv 11 \pmod{20}$, $x \equiv a \pmod{18}$

b) $2x \equiv a \pmod 3$, $3x \equiv 1 \pmod{10}$

■ 4 - ĐỊNH LÍ FERMAT VÀ ĐỊNH LÍ EULER

4.1- Định lí Fermat

Ta đã gặp bài toán sau đây (bài tập 1.11):

Chứng minh rằng với mọi số nguyên n:

a) $n^2 - n$ chia hết cho 2;

b) $n^3 - n$ chia hết cho 3;

c) $n^5 - n$ chia hết cho 5.

Bài toán này có thể giải được bằng cách phân tích

$n^2 - n$, $n^3 - n$, $n^5 - n$ ra thừa số.

a) $n^2 - n = n(n - 1)$. Trong hai số nguyên liên tiếp, $n - 1$ và n bao giờ cũng có một số chia hết cho 2.

b) $n^3 - n = n(n^2 - 1) = n(n - 1)(n + 1)$. Trong ba số nguyên liên tiếp, $n - 1$, n, $n + 1$, bao giờ cũng có một số chia hết cho 3.

c) $n^5 - n = n(n^4 - 1) = n(n^2 - 1)(n^2 + 1)$

$$= n(n-1)(n+1)(n^2+1).$$

Nếu n chia hết cho 5 thì $n^5 - n$ chia hết cho 5.

Nếu n không chia hết cho 5, thì n có dạng $5k \pm 1$ hoặc $5k \pm 2$ và trong ba số nguyên $n - 1$, $n + 1$ và $n^2 + 1$ luôn có một số chia hết cho 5:

- với $n = 5k + 1$ thì $n - 1 = 5k$, chia hết cho 5;

- với $n = 5k - 1$ thì $n + 1 = 5k$, chia hết cho 5;

- với $n = 5k \pm 2$ thì $n^2 = 25k \pm 20k + 4$ do đó $n^2 + 1 = 25k^2 \pm 20k + 5$, chia hết cho 5.

Ta chú ý rằng nếu như $n^2 - n \,\vdots\, 2$, $n^3 - n \,\vdots\, 3$, $n^5 - n \,\vdots\, 5$ với mọi số nguyên n, thì $n^4 - n$ không phải luôn luôn chia hết cho 4.

Thí dụ với n = 2, ta có $2^4 - 2 = 14$ không chia hết cho 4.

Các số 2, 3, 5 là các số nguyên tố và bài tập ta vừa giải là trường hợp riêng của định lí sau đây:

Định lí Fermat (Phec-ma)

Nếu p là số nguyên tố thì $n^p \equiv n \pmod p$

($n^p - n$ chia hết cho p) với mọi số nguyên n.

Thí dụ: $n^2 \equiv n \pmod 2$; $n^3 \equiv n \pmod 3$

$n^5 \equiv n \pmod 5$; $n^7 \equiv n \pmod 7$

$n^{11} \equiv n \pmod{11}$; $n^{13} \equiv n \pmod{13}$

Trong trường hợp p = 2,3, 5 ta có thể chứng minh bằng cách phân tích $n^p - n$ ra thừa số, nhưng rõ ràng là không thể áp dụng cách này cho số nguyên tố p bất kì.

Sau đây là một *cách chứng minh khác của định lí Fermat với p = 5.*

∇ Nếu n chia hết cho 5 thì hiển nhiên là $n^5 - n$ chia hết cho 5.

Xét n không chia hết cho 5. Lúc đó, 2n, 3n và 4n cũng đều không chia hết cho 5. Chia 4 số n, 2n, 3n, 4n cho 5, ta được 4 số dư đôi một khác nhau(vì nếu có hai số, thí dụ 4n và n, cho cùng số dư thì 4n - n = 3n sẽ chia hết cho 5), mỗi số dư lấy một trong bốn giá trị: 1,2,3,4. Thí dụ: nếu chia n cho 5 được số dư là 1, tức $n \equiv 1 \pmod 5$ thì $2n \equiv 2$, $3n \equiv 3$, $4n \equiv 4 \pmod 5$; nếu $n \equiv 2$ (modun 5) thì $2n \equiv 4$, $3n \equiv 6 \equiv 1$, $4n \equiv 8 \equiv 3 \pmod 5$.

Như vậy, ta có: $n \not\equiv 0 \pmod 5 \Rightarrow$

$$\begin{aligned} n &\equiv a \pmod 5 \\ 2n &\equiv b \pmod 5 \\ 3n &\equiv c \pmod 5 \\ 4n &\equiv d \pmod 5 \end{aligned}$$

Bốn số dư a,b,c,d đôi một khác nhau, mà mỗi số lấy một trong các giá trị 1,2,3,4, thế thì phải có

$a.b.c.d = 1.2.3.4$

Chú ý đến đẳng thức này, ta nhân từng vế bốn đồng dư thức trên đây và được:

$n.2n.3n.4n \equiv a.b.c.d \pmod 5$

$1.2.3.4.n^4 \equiv 1.2.3.4 \pmod 5$

Chia hai vế cho 1.2.3.4, nguyên tố với 5:

$$n^4 \equiv 1 \pmod 5$$

Nhân hai vế với n:

$n^5 \equiv n \pmod 5$. □

Tương tự như trên, ta chứng minh định lí Fermat với p nguyên tố bất kì.

∇ Nếu $n \equiv 0 \pmod p$ thì rõ ràng là $n^p \equiv n \pmod p$.

Nếu $n \not\equiv 0 \pmod p$ thì $2n, 3n, \dots, (p-1)n$ đều là $\not\equiv 0$ theo modun p, nghĩa là

$n \equiv a_1 \pmod p$ với $1 \le a_1 \le p-1$

$2n \equiv a_2 \pmod p$ với $1 \le a_2 \le p-1$

$3n \equiv a_3 \pmod p$ với $1 \le a_3 \le p-1$

....

$(p-1)n \equiv a_{p-1} \pmod p$ với $1 \le a_{p-1} \le p-1$.

p-1 số $a_1, a_2, a_3, \dots a_{p-1}$ (mỗi số lấy một trong các giá trị từ 1 đến p-1) là đôi một khác nhau, bởi vì nếu có hai số nào bằng nhau, thí dụ $a_k = a_h$ $(k > h)$ thì từ hai đồng dư thức trên đây mà vế phải là a_k và a_h,ta sẽ có $kn \equiv hn \pmod p$, do đó $(k-h)n \equiv 0 \pmod p$, trong đó $1 \le k-h \le p-1$, suy

ra n $\equiv$ 0 (mod p), trái với giả thiết.

Nếu p-1 số $a_1, a_2, a_3, \ldots a_{p-1}$ đôi một khác nhau, mà mỗi số lại lấy giá trị từ 1 đến p-1 thì tích của p-1 số đó phải bằng tích của các số từ 1 đến p-1:

$$a_1, a_2, a_3, \ldots a_{p-1} = 1.2.3\ldots(p-1).$$

Bây giờ ta nhân từng vế p-1 đồng dư thức trên đây và được:

$n.2n.3n\ldots.(p-1)n \equiv a_1 a_2 a_3 \ldots a_{p-1} \pmod p$

$n.2n.3n\ldots.(p-1)n \equiv 1.2.3(p-1) \pmod p$

$1.2.3\ldots.(p-1).n^{p-1} \equiv 1.2.3\ldots.(p-1) \pmod p$

Có thể chia hai vế của đồng dư thức cho tích 1.2.3....(p-1), nguyên tố với p, và được:

$$n^{p-1} \equiv 1 \pmod p$$

Từ đó $n^p \equiv n \pmod p$ □

4.2- Định lí Euler

Euler (Ơ le) đã mở rộng định lí Fermat cho trường hợp modun m bất kì và có định lí sau đây:

Nếu m là số nguyên dương bất kì và $\varphi(m)$ là số các số dương nhỏ hơn m và nguyên tố với m thì

$$N^{\varphi(m)} \equiv 1 \pmod m$$

với mọi số nguyên N nguyên tố với m.

Thí dụ 1- Cho m là số nguyên tố p. Tất cả các số dương nhỏ hơn p đều nguyên tố với p (có p-1 số từ 1 đến p-1), do đó $\varphi(p) = p - 1$; và nếu p nguyên tố thì mọi số nguyên không chia hết cho p đều là nguyên tố với p, và định lí Euler trở thành:

Nếu p là số nguyên tố thì $n^{p-1} \equiv 1 \pmod p$

với mọi số nguyên n không chia hết cho p.

Nhân hai vế của đồng dư thức với n, được

$$n^p \equiv n \pmod p$$

Đồng dư thức này đúng với mọi n không chia hết cho p, và đương nhiên cũng đúng với mọi n chia hết cho p, nghĩa là đúng với mọi n. Đó là định lí Fermat.

Thí dụ 2- Cho m = 8. Có tất cả 4 số dương nhỏ hơn 8 và nguyên tố với 8(đó là các số 1,3,5,và 7), nghĩa là $\varphi(8) = 4$. Theo định lí Euler:

$N^4 \equiv 1 \pmod 8$ với mọi N nguyên tố với 8.

Chú ý rằng $8 = 2^3$, nên N nguyên tố với 8 tức là N không chiá hết cho 2. Do đó, có thể phát biểu cách khác:

$N^4 - 1$ chia hết cho 8, với mọi số N lẻ.

Thí dụ 3- Cho m = 15. Có tất cả 8 số dương nhỏ hơn 15 và nguyên tố với 15(đó là: 1,2,4,7,8,11,13 và 14). Theo định lí Euler:

$N^8 \equiv 1 \pmod{15}$ với mọi N nguyên tố với 15.

Vì 15 = 3.5, nên N nguyên tố với 15 tức là N không là bội của 3 cũng không là bội của 5.

Sau đây, ta *chứng minh định lí Euler cho một trường hợp cụ thể*, chẳng hạn với m = 9.

∇ Nếu m = 9 thì có tất cả 6 số dương nhỏ hơn 9 và nguyên tố với 9(các số: 1,2,4,5,7 và 8), nghĩa là $\varphi(9) = 6$.

Bất cứ số N nào nguyên tố với 9 thì khi chia cho 9 sẽ cho số dư là một số dương nhỏ hơn 9 và nguyên tố với 9, nghĩa là N đồng dư (theo mod 9) với một trong 6 số: 1,2,4,5,7 hoặc 8. Nếu ta nhân N với một số nguyên tố với 9(thí dụ: 2,4,5,7,8) thì tích cũng là một số nguyên tố với 9, do đó tích cũng phải đồng dư(theo mod 9) với một trong 6 số nói trên. Như vậy:

$N \equiv a \pmod 9$

$2N \equiv b \pmod 9$

$4N \equiv c \pmod 9$

$5N \equiv d \pmod 9$

$7N \equiv e \pmod 9$

$8N \equiv g \pmod 9$

(a,b,c,d,e,g là một trong 6 số: 1,2,4,5,7,8)

Sáu số a,b,c,d,e,g đôi một khác nhau, vì nếu có hai số bằng nhau, thí dụ $b = g$ thì từ hai đồng dư thức thứ hai và thứ sáu trên đây, sẽ có $2N \equiv 8N \pmod 9$, hay $8N - 2N = 6N \equiv 0 \pmod 9$, tức $N \equiv 0 \pmod 9$, mâu thuẫn với giả thiết là N nguyên tố với 9.

Sáu số a,b,c,d,e,g đôi một khác nhau và mỗi số lấy một trong các giá trị 1,2,4,5,7,8, như vậy tích a.b.c.d.e.g phải bằng tích 1.2.4.5.7.8:

$$a.b.c.d.e.g = 1.2.4.5.7.8$$

Chú ý đến đẳng thức này, ta nhân từng vế sáu đồng dư thức ở trên và được:

$$N.2N.4N.5N.7N.8N \equiv a.b.c.d.e.g \pmod 9$$

$$1.2.4.5.7.8.N^6 \equiv 1.2.4.5.7.8 \pmod 9$$

Chia hai vế cho 1.2.4.5.7.8, nguyên tố với 9, được:

$$N^6 \equiv 1 \pmod 9$$

trong đó $6 = \varphi(9)$ và N là số bất kì, nguyên tố với 9. ❐

Chú ý rằng $9 = 3^2$, trường hợp riêng trên đây của định lí Euler có thể phát biểu:

$N^6 - 1$ chia hết cho 9, với mọi N không phải là bội của 3 (xem bài tập 1.12b).

Có thể mở rộng dễ dàng cách chứng minh với $m = 9$ trên đây để chứng minh tổng quát định lí Euler, với $m > 0$ bất kì.

Bạn đọc có thể thấy rằng cách chứng minh tương tự với chứng minh của định lí Fermat.

Công thức tính giá trị của $\varphi(m)$

Trong trường hợp m nhỏ, có thể liệt kê các số dương nhỏ hơn m và nguyên tố với m để biết giá trị của $\varphi(m)$. Người ta chứng minh được công thức sau đây của $\varphi(m)$:

Giả sử m được phân tích thành thừa số nguyên tố

$m = p_1^{m_1} p_2^{m_2} .. p_k^{m_k}$ trong đó $p_1, p_2, ... p_k$ là các số nguyên tố đôi một khác nhau.

Thế thì:

$$\varphi(m) = m(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \dots (1 - \frac{1}{p_k})$$

Thí dụ:

$$m = 9 = 3^2 \Rightarrow \varphi(9) = 9(1 - \frac{1}{3}) = 6$$

$$m = 12 = 2^2.3 \Rightarrow \varphi(12) = 12(1 - \frac{1}{2})(1 - \frac{1}{3}) = 4$$

$$m = 15 = 3.5 \Rightarrow \varphi(15) = 15(1 - \frac{1}{3})(1 - \frac{1}{5}) = 8$$

$$m = 20 = 2^2.5 \Rightarrow \varphi(20) = 20(1 - \frac{1}{2})(1 - \frac{1}{5}) = 8$$

Người ta đã lập bảng cho giá trị của $\varphi(m)$ ứng với mọi m ≤ 10000 và bảng cho giá trị của m ứng với $\varphi(m) \le 2500$. Người ta thấy rằng trong phạm vi các bảng đó, bao giờ cũng có ít nhất hai giá trị khác nhau của m cho cùng một giá trị của $\varphi(m)$. Thí dụ: $\varphi(3) = \varphi(4) = \varphi(6) = 2$, $\varphi(5) = \varphi(8) = 4$. Nhưng liệu có kết quả tổng quát sau đây hay không: Với mọi số tự nhiên m bao giờ

cũng có một số tự nhiên $m' \neq m$ sao cho $\varphi(m) = \varphi(m')$? Cho đến nay, chưa có ai chứng minh hay bác bỏ được điều này !

Một số thí dụ áp dụng

Thí dụ 1- Tìm số dư trong phép chia 3^{100} cho 13.

∇ Vì 13 là số nguyên tố, theo định lí Fermat ta có:

$$3^{12} \equiv 1 \pmod{13}$$

Mà $100 = 12.8 + 4$ nên $3^{100} = (3^{12})^8 . 3^4 \equiv 3^4 \pmod{13}$

Nhưng $3^4 = 81 \equiv 3 \pmod{13}$

suy ra số dư trong phép chia 3^{100} cho 13 là 3. ❐

Thí dụ 2- Giải phương trình đồng dư

$$7x \equiv 3 \pmod{27} \quad (1)$$

∇ Vì $(7,27) = 1$, theo định lí Euler ta có: $7^{\varphi(27)} \equiv 1 \pmod{27}$.

Mà $\varphi(27) = 27(1 - \frac{1}{3}) = 18$ nên $7^{18} \equiv 1 \pmod{27}$ (2)

Nhân hai vế của (2) với 3 và viết 7^{18} thành 7.7^{17}, được

$$7.(7^{17}.3) \equiv 3 \pmod{27} \quad (3)$$

So sánh (1) với (3), được

$$x \equiv 7^{17}.3 \pmod{27} \quad (4)$$

Ta có $7^2 \equiv -5 \pmod{27}$ $\quad 7^4 \equiv (-5)^2 \equiv -2 \pmod{27}$

Mà $17 = 4.4 + 1$, nên $7^{17} \equiv (7^4)^4 . 7 \equiv (-2)^4.7 \pmod{27}$

$$7^{17} \equiv 16.7 \equiv 4 \pmod{27}$$

Thay vào (4), được: $x \equiv 12 \pmod{27}$ ❐

Thí dụ 3- Chứng minh rằng trong các số tự nhiên thế nào cũng có số k sao cho $1983^k - 1$ chia hết cho 10^5. (Đề thi học sinh giỏi toán cấp II toàn quốc, 1983)

∇ Vì 1983 không chia hết cho 3 và không chia hết cho 5, còn $10^5 = 2^5 . 5^5$ nên $(1983, 10^5) = 1$, do đó có thể áp dụng định

lí Euler và có

$$1983^{\varphi(10^5)} \equiv 1 \pmod{10^5}$$

$$\text{Mà } \varphi(10^5) = 10^5\left(1-\frac{1}{2}\right)\left(1-\frac{1}{5}\right) = 4.10^4,$$

và đây là số k cần tìm. □

Nếu không biết đến định lí Euler thì bài toán có thể giải như sau:

∇ Cho k lần lượt lấy $10^5 + 1$ giá trị liên tiếp, từ 1 trở đi, ta được $10^5 + 1$ giá trị khác nhau của $1983^k - 1$.

Chia $10^5 + 1$ số này cho 10^5, ta có nhiều nhất là 10^5 số dư, do đó theo nguyên tắc Dirichlet phải có ít nhất hai số cho cùng số dư. Giả sử đó là số $1983^m - 1$ và $1983^n - 1$ $(m>n)$. Thế thì hiệu của hai số này phải chia hết cho 10^5:

$(1983^m - 1) - (1983^n - 1)$ chia hết cho 10^5.

$$\text{Mà } (1983^m - 1) - (1983^n - 1) = 1983^m - 1983^n = 1983^n(1983^{m-n} - 1)$$

Nhưng 1983^n và 10^5 nguyên tố cùng nhau, do đó phải có $1983^{m-n} - 1$ chia hết cho 10^5. Như vậy là có số $k' = m - n$ sao cho $1983^{k'} - 1$ chia hết cho 10^5. □

Chú ý rằng với cách giải thứ nhất *(dùng định lí Euler)* thì chỉ ra được rằng với $k = 40000$ thì $1983^k - 1$ chia hết cho 10^5. Với cách giải thứ hai, dùng *nguyên tắc Dirichlet*, tức là chứng minh bằng phản chứng, ta chỉ chứng minh được rằng có một số k thỏa mãn yêu cầu của bài toán (không có số k đó thì vô lí), chứ không chỉ ra dược cụ thể số k đó bằng bao nhiêu.

Bài tập

1.71- Tìm số gồm toàn chữ số 9 và chia hết cho : 3; 7; 11; 13; 17.

1.72- Chứng minh rằng

$$1^{4k} + 2^{4k} + 3^{4k} + 4^{4k} \text{ không chia hết cho } 5.$$

1.73- Chứng minh rằng nếu

$$a_1 + a_2 + \ldots + a_n \equiv 0 \pmod{30}$$

thì $$a_1^5 + a_2^5 + \ldots + a_n^5 \equiv 0 \pmod{30}.$$

1.74- Chứng minh rằng nếu $(a,240) = 1$ thì

$$a^4 \equiv 1 \pmod{240}.$$

1.75- Chứng minh rằng nếu p là số nguyên tố > 7 thì

$$3^p - 2^p - 1 \,\vdots\, 42p\,.$$

1.76- a) Tìm tất cả các số tự nhiên n sao cho $n \mid 2^n - 1$.

b) Tìm tất cả các số nguyên tố p sao cho $p \mid 2^p + 1$.

1.77- Chứng minh rằng nếu n lẻ thì $2^{n!} - 1 \,\vdots\, n$.

1.78- Cho m và n là hai số tự nhiên >1 và nguyên tố cùng nhau. Chứng minh rằng:

$$m^{\varphi(n)} + n^{\varphi(m)} \equiv 1 \pmod{mn}\,.$$

1.79- Chứng minh rằng với mỗi số nguyên tố p có vô số số có dạng $2^n - n$ (n là số tự nhiên) chia hết cho p.

1.80- Chứng minh rằng

$$1^{30} + 2^{30} + \ldots + 10^{30} \equiv -1 \pmod{11}.$$

CHƯƠNG 2

SỐ NGUYÊN TỐ

Chúng ta đều biết rằng:

Số nguyên tố là số lớn hơn 1 và chỉ có hai ước số là 1 và chính nó. Thí dụ: 2, 3, 5, 7, 11, ...

Hợp số là số lớn hơn 1 và có nhiều hơn hai ước số. Thí dụ: 4 (có ba ước số: 1,2, và 4), 10 (có bốn ước số: 1,2,5và 10).

Số 1 và số 0 đều không phải là số nguyên tố mà cũng không phải là hợp số (số 1 chỉ có một ước số, số 0 có vô số ước số).

Số nguyên tố đóng vai trò trung tâm trong số học, do định lí sau đây:

Định lí cơ bản của số học

Mọi số lớn hơn 1 đều phân tích được ra thừa số nguyên tố một cách duy nhất (không kể thứ tự các thừa số).

Thí dụ: 60 = 5.2.3.2 = 2.2.3.5.

Các tích có được *chỉ khác nhau về thứ tự các thừa số nguyên tố mà thôi* . Người ta thường phân tích một số ra thừa số *dưới dạng tiêu chuẩn,* trong đó *các thừa số nguyên tố được sắp xếp theo thứ tự từ nhỏ đến lớn,* mỗi thừa số với số mũ tương ứng. Thí dụ: $60 = 2^2.3.5$, $525 = 3.5^2.7$.

Chung quanh các số nguyên tố có nhiều kết quả thú vị và còn rất nhiều bí ẩn. Nhiều bài toán, nhiều dự đoán được phát biểu rất đơn giản, nhưng việc chứng minh thường rất phức tạp, phải dùng đến những công cụ tinh vi của toán học cao cấp và không ít bài toán hàng trăm năm nay vẫn chưa có lời giải.

Sau đây là mấy bài toán đơn giản.

1- Có bao nhiêu số nguyên tố?

Ngay từ thời thượng cổ, nhà toán học Euclide (Ơ-clit) đã chứng minh được rằng:

Có vô số số nguyên tố; dãy số nguyên tố

2,3,5,7,11,13,17,...

có thể kéo dài vô hạn, nói cách khác, *không có số nguyên tố nào là lớn nhất.*

Để chứng minh định lí này, Euclide đã có một suy nghĩ rất hay: nhân một số số nguyên tố đầu tiên với nhau, rồi cộng kết quả có được với 1, ta có:

$$2.3 + 1 = 7$$
$$2.3.5 + 1 = 31$$
$$2.3.5.7 + 1 = 211$$
$$2.3.5.7.11 + 1 = 2311$$
$$2.3.5.7.11.13 + 1 = 30031$$
....

Mỗi số có được trong vế phải của các đẳng thức trên đây đều không chia hết cho bất kì số nguyên tố nào trong tích ở vế trái tương ứng. Thí dụ: số 31 không chia hết cho 2, 3 hay 5 (chia cho 2,3,5 bao giờ cũng có số dư là 1), số 2311 không thể chia hết cho 2,3,5,7 hay 11. Và cũng rõ ràng là mỗi số trong vế phải của các đẳng thức trên đây đều lớn hơn số nguyên tố lớn nhất trong tích ở vế trái tương ứng. Ta có:

Các số 7, 31, 211, 2311 đều là số nguyên tố (chú ý: 7 > 3, 31 > 5, 211 > 11) , còn số 30031 là hợp số, là tích của hai số nguyên tố: 30031 = 59.509, cả hai số nguyên tố 59 và 509 đều lớn hơn 13.

Bây giờ, ta hiểu dễ dàng chứng minh sau đây của định lí: không có số nguyên tố nào là lớn nhất.

∇ Ta lấy một số nguyên tố p bất kì. Lập tích của p với tất cả các số nguyên tố nhỏ hơn p rồi cộng thêm 1, ta được số N:

$$2.3.5.7.11...p + 1 = N$$

Có hai khả năng:

1) N là số nguyên tố. Đây là số nguyên tố > p (thí dụ: p = 7 thì N = 211 > 7).

2) N là hợp số. Chia N cho 2, 3, 5,...p ta luôn có số dư là 1, do dó nếu phân tích N ra thừa số nguyên tố thì các thừa số nguyên tố này đều lớn hơn p (thí dụ: với p = 13 thì N = 599.509).

Như vậy, với mọi số nguyên tố p đều có số nguyên tố lớn hơn nó, nghĩa là không có số nguyên tố nào là lớn nhất. □

Cũng có thể chứng minh khác chút ít, *bằng phản chứng:*

∇ Giả sử có p là số nguyên tố lớn nhất. Ta lập số

$$2.3.5.7.11...p + 1 = N$$

Số N không chia hết cho bất kì số nguyên tố nào (vì chia cho 2,3,5,7,...cho đến số nguyên tố lớn nhất là p, thì luôn có số dư là 1), do đó N phải là số nguyên tố. Nhưng N > p, mà theo giả thiết, p đã là số nguyên tố lớn nhất, nên N phải là hợp số. Như vậy, nếu giả sử có số nguyên tố p là lớn nhất thì ta sẽ đi đến mâu thuẫn: số N vừa là số nguyên tố, vừa là hợp số. □

Sàng Euratosthène (Ơratôtsten)

Có vô số số nguyên tố, nhưng các số nguyên tố được sắp xếp như thế nào trong tập hợp các số tự nhiên thì cho đến nay

người ta chưa tìm ra được một qui luật gì. Người ta đã lập bảng các số nguyên tố không vượt quá một số nào đó. Sàng Euratosthène là một phương pháp đơn giản để lập bảng này (Euratosthène là một nhà bác học cổ Hi Lạp, sống vào thế kỉ thứ 3 trước công nguyên, cùng thời với Euclide). Ta dựa vào định lí sau đây:

Định lí- *Ước số nguyên tố nhỏ nhất của một hợp số N là một số không vượt quá $\sqrt{N}$.*

Thí dụ: $35 = 5.7$, ước nguyên tố nhỏ nhất của 35 là 5, mà $5 = \sqrt{25} < \sqrt{35}$.

∇ Gọi p là ước nguyên tố nhỏ nhất của N, tức là $N = pN_1$, với $p < N_1$, do đó $p.p < p.N_1$ hay $p^2 < N$, suy ra $p < \sqrt{N}$. ❒

Hệ quả- *Nếu số $N > 1$ không có một ước nguyên tố nào từ 2 cho đến $\sqrt{N}$ thì N là một số nguyên tố.*

Thí dụ- Cho số 139. Ta có $11^2 = 121 < 139 < 144 = 12^2$, do đó $11 < \sqrt{139} < 12$ và các số nguyên tố từ 2 đến không quá $\sqrt{139}$ là 2, 3, 5, 7, 11. Số 139 không chia hết cho số nào trong năm số nguyên tố này, vậy 139 là số nguyên tố.

Ta dựa vào định lí trên để lập bảng các số nguyên tố không vượt quá một số N cho trước.

Thí dụ lấy $N = 50$. Ta viết tất cả các số tự nhiên từ 2 đến 50,rồi xóa đi tất cả các hợp số, chỉ giữ lại các số nguyên tố như sau:

Số 2 là số nguyên tố, ta giữ số 2 lại và xóa đi tất cả các bội của 2, đó là các số tận cùng bằng 2 (trừ số 2), 4, 6, 8, 0; ta gạch các số này bằng *đường gạch đứng.*

Số đầu tiên sau số 2 không bị xóa là số 3. Số 3 là số nguyên tố (nếu không thì nó sẽ có ước nguyên tố nhỏ hơn nó là số 2

và nó đã bị xóa đi rồi).Ta giữ số 3 lại và xóa đi tất cả bội của 3, là các số 6,9,12,...Ta xoá các số này bằng *đường gạch chéo* (số 6,12 ... bị xóa lần thứ hai, vì vừa là bội của 2, vừa là bội của 3).

	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50

Số đầu tiên sau số 3 không bị xóa là số 5. Số 5 là số nguyên tố. Ta giữ số 5 lại và xóa đi tất cả các bội của 5, đó là các số tận cùng bằng 0 (đã bị xoá) và các số tận cùng bằng 5 ; ta xoá cột số này (trừ số 5) bằng *đường gạch đứng hai nét.*

Số đầu tiên sau số 5 không bị xóa là số 7. Số 7 là số nguyên tố, ta giữ 7 lại và xoá đi tất cả các bội khác của 7; chỉ cần xoá thêm 7.7 = 49 (các bội khác của 7, cũng là bội của 2, 3, 5 đã được xoá trước rồi).

Đến đây ta dừng lại: mọi số trong bảng (từ 2 đến 50) không bị xóa đều là số nguyên tố. Thực vậy, trong bảng không còn một hợp số nào, vì theo định lí trên đây, mọi hợp số ≤ 50 có ước nhỏ nhất là số nguyên tố $\leq \sqrt{50}$, tức ≤ 7 và do đó đã được xóa đi rồi. Như vậy, ta có tất cả là 15 số nguyên tố ≤ 50, đó là

2,3,5,7,11,13,17,19,23,29,31,37,41,43,47.

Từ bảng các số nguyên tố ≤ 50, dựa vào hệ quả của định lí trên đây, ta có thể xác định được rằng mỗi số tự nhiên $a \leq 50^2 = 2500$ có phải là nguyên tố hay không. Muốn vậy, ta phải thử xem số $a > 1$ đó có ước nguyên tố nào $\leq \sqrt{a}$ không, nếu không có thì a là số nguyên tố. *Thí dụ:* với số 211 thì

$\sqrt{211} < 17$;các số nguyên tố nhỏ hơn 17 là 2,3,5,7,11,13,đều không phải là ước số của 211, nên 211 là số nguyên tố; xét số 1139, ta có $1139 < 1369 = 37^2$ vì vậy ta thử chia 1139 lần lượt cho các số nguyên tố từ 2 đến 31 (<37), ta thấy 1139 chia hết cho 17, cho nên 1139 không phải là nguyên tố (1139 = 17.67).

Trong thực tế, muốn biết một số nào đó (không lớn lắm) có phải là nguyên tố hay không, người ta tìm xem nó có mặt hay không trong bảng các số nguyên tố đã lập sẵn. Người ta đã lập bảng cho tới 100 triệu số nguyên tố đầu tiên.

Tuy nhiên, với một số A rất lớn, vượt ra ngoài bảng các số nguyên tố đã lập, việc xác định A có là số nguyên tố hay không là vấn đề không đơn giản, vì phải thực hiện rất nhiều phép tính. Cho đến 1985, số nguyên tố lớn nhất mà người ta biết được là số $2^{132049} - 1$, gồm 39751 chữ số trong hệ ghi số thập phân (chú ý rằng số một tỉ chỉ gồm có 10 chữ số!).

Gần đây, hai sinh viên Mĩ đã tìm ra một số nguyên tố lớn hơn nữa, đó là số $2^{216091} - 1$, gồm 65050 chữ số ! Họ đã bỏ ra khoảng ba năm làm việc trên máy tính điện tử để đi đến kết quả này.

1.3 - Qua bảng các số nguyên tố đã lập dược, người ta thấy rằng có những cặp số nguyên tố rất gần nhau, hiệu giữa chúng chỉ bằng 2, thí dụ 3 và 5, 5 và 7, 11 và 13, 191 và 193, 2711 và 2713. Những cặp số như vậy được gọi là *cặp số nguyên tố sinh đôi*. Từ 1 đến 30 triệu có 152892 cặp số nguyên tố sinh đôi. Tuy nhiên, cho đến nay, người ta chưa biết được là có hữu hạn hay vô số cặp số nguyên tố sinh đôi (có hay không có cặp số nguyên tố sinh đôi lớn nhất); chỉ biết rằng có những cặp số sinh đôi rất lớn, thí dụ như: 10 006 427 và

10 006 429, 1000 000 009 549 và 1000 000 009 551.

Trong khi đó,có thể chỉ ra được một dãy nhiều bao nhiêu cũng được các số tự nhiên liên tiếp, trong đó không có một số nguyên tố nào.

Thực vậy, cho một số k tùy ý. Ta lập tích của tất cả các số từ 1 đến k,kí hiệu tích đó là k! (đọc : k giai thừa):

$$k! = 1.2.3....(k-1).k$$

Thí dụ: 2! = 1.2 = 2, 3! = 1.2.3 = 6

4! = 1.2.3.4= 24, 5! = 1.2.3.4.5 = 120

6! = 1.2.3.4.5.6 = 720

Thế thì k - 1 số liên tiếp sau đây đều là hợp số:

k! + 2 (chia hết cho 2)

k! + 3 (chia hết cho 3)

..... k! + k (chia hết cho k)

Thí dụ với k = 6 thì 5 số liên tiếp sau đây đều là hợp số:

6! + 2 = 720 + 2 = 722,

6! + 3 = 723 ,

6! + 4 = 724,

6! + 5 = 725

và 6! + 6 = 726.

Lấy k = 1001 thì ta có 1000 số liên tiếp là hợp số:

1001! + 2 ,

1001! + 3 ,

...1001! + 1000

Lấy $k = 10^6 + 1$ thì có 10^6(một triệu) số liên tiếp là hợp số:

$(10^6 + 1)! + 2$,

$(10^6 + 1)! + 3$,

...

$(10^6 + 1)! + 10^6$,

$(10^6 + 1)!\ 10^6 + 1$.

Chú ý rằng k! tăng lên rất nhanh khi k tăng: 2! = 2, 6! = 720,...,10! = 1.2.3.4.5.6.7.8.9.10 = 3628800, cho nên 1001!, $(10^6 + 1)!$ là những số rất lớn.

Kết quả trên đây cũng cho ta hình dung được rằng các số nguyên tố được phân phối tương đối thưa thớt dần trong dãy các số tự nhiên . Qua bảng các số nguyên tố, ta thấy: từ 1 đến 10 có 4 số nguyên tố (2,3,5,7), số nguyên tố chiếm tỉ lệ 4/10 = 0,4 = 40%; từ 1 đến 100 có 25 số nguyên tố (chiếm tỉ lệ 25/100 = 25% = 0,25), từ 1 đến 1000 có 168 số nguyên tố (tỉ lệ xấp xỉ 17% = 0,17),...,từ 1 đến 10^6(một triệu) có 78498 số nguyên tố(tỉ lệ xấp xỉ 8% = 0,08).

Gọi $\pi(n)$ là số các số nguyên tố không vượt quá n thì tỉ số $\frac{\pi(n)}{n}$ giảm dần khi n tăng:

$$\frac{\pi(10)}{10} = 0,4, \qquad \frac{\pi(100)}{100} = 0,25;$$

$$\frac{\pi(1000)}{1000} = 0,17; \quad \frac{\pi(10^6)}{10^6} = 0,08;...$$

Euler đã chứng minh được rằng $\frac{\pi(n)}{n}$ dần tới 0 khi n tăng vô cùng. Tuy nhiên, về bản thân số $\pi(n)$ thì người ta còn biết quá ít, việc nghiên cứu nó là vấn đề còn rất khó khăn.

2- Có bao nhiêu số nguyên tố có dạng ax + b?

Trên đây, ta đã chứng minh rằng có vô số số nguyên tố. Số 2 là số nguyên tố chẵn duy nhất, còn tất cả các số nguyên tố khác đều là số lẻ. Tập hợp số nguyên tố là vô hạn; nếu không kể số 2, thì tập hợp đó cũng là vô hạn.Vì vậy, có thể nói: có vô số số nguyên tố lẻ.

Mỗi số lẻ đều có dạng $2x + 1$ (với $x \geq 0$) hoặc $2x - 1$ (với $x \geq 1$). Do đó, cũng có thể nói rằng:

Có vô số số nguyên tố dạng $2x - 1$ ($x \geq 1$).

hay là: Có vô số số nguyên tố trong dãy số lẻ:

1,3,5,7,9,11,13,15...

Từ cách phát biểu này, có thể đặt vấn đề: có hay không có kết quả tương tự sau đây:

Có vô số số nguyên tố dạng $3x - 1$ ($x \geq 1$) ?

hay là: có vô số số nguyên tố trong dãy số sau đây: 2,5,8,11,14,17,20,..

(số đầu tiên của dãy là 2, ứng với $x = 1$, $3x - 1 = 2$; số tiếp theo bằng số đứng trước cộng thêm 3: $2 + 3 = 5$, $5 + 3 = 8$,...)

Dự đoán này là đúng, có thể chứng minh như sau:

∇ Trước hết, lưu ý rằng mọi số ≥ 2 đều có một trong các dạng: $3x$ (thí dụ: $6 = 3.2$, $21 = 3.7$) hoặc $3x + 1$ (thí dụ: $7 = 3.2 + 1$, $22 = 3.7 + 1$) hoặc $3x - 1$(thí dụ: $2 = 3.1 - 1$, $23 = 3.8 - 1$). Mặt khác, tích của hai số có dạng $3x + 1$ cũng là một số có dạng $3x + 1$. Thực vậy, lấy hai số $3m + 1$ và $3q + 1$, ta có:

$$(3m + 1)(3q + 1) = 9mq + 3m + 3q + 1$$
$$= 3(3mq + m + q) + 1$$

và đây là một số có dạng $3x + 1$.

Bây giờ, ta lấy một số nguyên tố p bất kì, có dạng 3x – 1. Lập tích của p với tất cả các số nguyên tố nhỏ hơn p, rồi trừ đi 1, ta được số M:

$$\underbrace{2.3.5.7.11...p}_{\text{bội của 3}}-1 = M$$

M là một số có dạng 3x – 1.

Có hai khả năng:

1) M là số nguyên tố. Đó là số nguyên tố có dạng 3x - 1 và lớn hơn p.

2) M là hợp số. Chia M cho 2, 3, 5,..., p ta luôn có số dư là 1, do đó các ước số nguyên tố của M đều lớn hơn p. Trong các ước số nguyên tố này không thể có số nào có dạng 3x (là hợp số) và không thể tất cả đều có dạng 3x + 1(vì như vậy thì M sẽ có dạng 3x + 1), do đó ít nhất một trong các ước số nguyên tố của M phải có dạng 3x – 1.

Như vậy, trong mọi trường hợp đều có một số nguyên tố có dạng 3x– 1 và lớn hơn p, hoặc đó là số M hoặc đó là một ước số nguyên tố của M. Điều đó chứng tỏ *không có số nguyên tố dạng 3x – 1 là lớn nhất, nghĩa là có vô số số nguyên tố dạng 3x – 1.* □

Chú ý rằng số có dạng 3x– 1 (x ≥ 1) cũng là số có dạng 3x + 2 (x ≥ 0).

Có thể thấy rằng chứng minh trên đây tương tự chứng minh của Euclide về định lí"có vô số số nguyên tố". Và cũng với ý của chứng minh này, có thể chứng minh rằng: có vô số số nguyên tố dạng 4x+ 3, dạng 6x + 5,...Tuy nhiên việc chứng minh rằng có vô số số nguyên tố dạng 3x + 1, 4x + 1 thì phức tạp hơn nhiều.

Trên đây là những trường hợp riêng của định lí sau đây:

Có vô số số nguyên tố có dạng $ax + b$, với a,b nguyên tố cùng nhau.

Định lí này được nhà toán học Đức *Dirichlet* (Đi-rích-sơ-lê, 1805- 1859) chứng minh năm 1837. Chứng minh của Direchlet dùng đến những kiến thức của toán học cao cấp. Mãi 112 năm sau, năm 1949, nhà toán học Na Uy Selberg (Xenbec,sinh năm 1917) mới tìm được một chứng minh sơ cấp (nhưng rất phức tạp!) của định lí này.

Chú ý rằng $ax+b$ là một nhị thức bậc nhất. Đương nhiên là người ta nghĩ đến những số nguyên tố có dạng phức tạp hơn. Nhưng đây là một vấn đề rất khó khăn. Chẳng hạn như,có thể chỉ ra rất nhiều số nguyên tố dạng $x^2 + 1$:

2 (với $x = 1$), 5 (với $x = 2$), 17 (với $x = 4$), 101 (với $x = 10$), 197 (với $x = 14$),...

(với $x \leq 100000$, có 6656 số nguyên tố dạng $x^2 + 1$). Người ta dự đoán rằng có vô số số nguyên tố dạng này, nhưng cho đến nay, đây vẫn là một bài toán hết sức khó, đang chờ người giải ! Tương tự như vậy với những số nguyên tố có dạng $x^3 + 2$, $x^3 - 2$,...

■3 - Có bao nhiêu số hoàn chỉnh?

Từ thượng cổ, các nhà toán học Hi Lạp trong khi đi tìm "vẻ đẹp" của các con số, đã chú ý đến hai số 6 và 28, có tính chất rất đặc biệt: mỗi số bằng nửa tổng các ước số của nó. Số 6 có các ước số là 1,2,3 và 6:

$$(1 + 2 + 3 + 6) : 2 = 6.$$

Số 28 có các ước số là 1, 2, 4, 7, 14, 28 và ta có:

$$(1 + 2 + 4 + 7 + 14 + 28) : 2 = 28.$$

Ta gọi *số hoàn chỉnh là số bằng nửa tổng các ước số của nó*. Cũng có thể nói: số hoàn chỉnh là số bằng tổng các ước số của nó, không kể bản thân nó. (6 = 1 + 2 + 3, 28 = 1 + 2 + 4 + 7 + 14).

Các nhà toán học cổ Hi Lạp thấy rằng các số hoàn chỉnh là rất hiếm hoi, họ chỉ tìm ra được hai số hoàn chỉnh nữa là 496 và 8128. Ta hãy kiểm tra lại xem hai số này có đúng là số hoàn chỉnh hay không. Muốn vậy, ta phải liệt kê các ước số của chúng sao cho đủ không dư, không sót) và có thể tính tổng của chúng được thuận lợi.

∇ Ta phân tích số N = 496 thành thừa số nguyên tố:

$$N = 496 = 2^4.31.$$

Các ước số của 496 có thể liệt kê như sau:

1	2 2^2	2^3	2^4	
31	2.31	$2^2.31$	$2^3.31$	$2^4.31$.

Đó là tất cả các ước số của 496, không sót số nào. Tổng S các ước số này là

$$S = (1+2+2^2+2^3+2^4)+(1+2+2^2+2^3+2^4).31$$
$$= (1 + 2 + 2^2 + 2^3 + 2^4)\ (1 + 31).$$

Ta tính riêng $s = 1 + 2 + 2^2 + 2^3 + 2^4$.

Chú ý rằng $2s = 2 + 2^2 + 2^3 + 2^4 + 2^5$

ta có $2s - s = s = 2^5 - 1$.

Do đó $S = (2^5 - 1)(1 + 31)$.

Chú ý rằng $1 + 31 = 32 = 2^5$ và $2^5 - 1 = 31$

ta có $S = (2^5 - 1)(1 + 31) = 31.2^5 = 2(2^4.31) = 2N$

nghĩa là $N = 496 = 2^4.31$ là số hoàn chỉnh. □

Tương tự như vậy, có thể kiểm tra được rằng

$$N = 8128 = 2^6.127 \text{ là số hoàn chỉnh.}$$

∇ Thực vậy, tổng S các ước số của 8128 là

$S = (1+2+2^2+2^3+2^4+2^5+2^6)(1+127) = (2^7 - 1)(1 + 127).$

Mà $1 + 127 = 2^7$, nên $S = 2^7.127 = 2(2^6.127) = 2N$. □

Với bốn số hoàn chỉnh là 6,28,496,8128, chú ý rằng:

$$6 = 2.3 \qquad 28 = 2^2.7$$

$$496 = 2^4.31 \qquad 8128 = 2^6.127$$

trong đó 3,7,31 và 127 đều là số nguyên tố, Euclide đã tìm các số hoàn chỉnh trong những số N có dạng tổng quát là

$$N = 2^k.p \ (k \geq 1, \text{ p nguyên tố}).$$

Có thể liệt kê tất cả các ước số của $N = 2^k.p$ như sau:

$$\begin{array}{llll} 1 & 2 & 2^2 \ldots 2^{k-1} & 2^k \\ p & 2.p & 2^2.p \ldots 2^{k-1}.p & 2^k.p \end{array}$$

Tổng S các ước số này là:

$$S = (1+2+2^2+\ldots+2^{k-1}+2^k) + p(1+2+2^2+\ldots+2^{k-1}+2^k =$$
$$= (1+2+2^2+\ldots+2^{k-1}+2^k)(1 + p)$$

Để tính $s = 1 + 2 + 2^2 + \ldots + 2^{k-1} + 2^k$

ta chú ý rằng $2s = 2 + 2^2 + \ldots + 2^k + 2^{k+1}$

do đó $2s - s = s = 2^{k+1} - 1$

và có $\qquad S = (2^{k+1} - 1)(1 + p).$

S là tổng các ước số của $N = 2^k.p$. Theo định nghĩa, N là số hoàn chỉnh khi và chỉ khi $S = 2N$, tức là

$$(2^{k+1} - 1)(1 + p) = 2.2^k.p$$

hay $\quad 2^{k+1} + 2^{k+1}.p - 1 - p = 2^{k+1}.p$ suy ra $p = 2^{k+1} - 1$.

Như vậy ta đã chứng minh được rằng:

Số N $= 2^k.p$ (p nguyên tố, $k \geq 1$) là số hoàn chỉnh khi và chỉ khi $p = 2^{k+1} - 1$.

Nói cách khác, số $N = 2^k(2^{k+1} - 1)$, với $k \geq 1$) là số hoàn chỉnh khi và chỉ khi $2^{k+1} - 1$ là số nguyên tố.

Đặt $n = k + 1$ thì $N = 2^k(2^{k+1} - 1)$ với $k \geq 1$

có dạng $N = 2^{n-1}(2^n - 1)$ với $n \geq 2$.

Kết quả này đã được biết từ thời Euclide (thế kỉ thứ 3 trước công nguyên); Euler (1707 - 1783) đã chứng minh tiếp rằng: mọi số hoàn chỉnh chẵn đều phải có dạng trên đây, do đó ta có định lí:

Định lí- Một số chẵn là số hoàn chỉnh khi và chỉ khi nó có dạng $2^{n-1}(2^n - 1)$ trong đó $2^n - 1$ ($n \geq 2$) là số nguyên tố.

Như vậy, việc tìm số hoàn chỉnh chẵn gắn với việc tìm số n sao cho $2^n - 1$ là số nguyên tố. Số nguyên tố có dạng $2^n - 1$ được gọi là số nguyên tố Mersenne (Mec-xen, 1588-1648, một tu sĩ người Pháp, đã dày công nghiên cứu về số hoàn chỉnh).

Có thể chứng minh rằng nếu n là hợp số thì 2^n-1 cũng là hợp số. Nhưng không phải cứ n là số nguyên tố thì $2^n - 1$ là số nguyên tố, thí dụ với $n = 11$ thì $2^{11} - 1 = 2047 = 23.89$.

Mỗi số nguyên tố Mersenne cho ta một số hoàn chỉnh chẵn. Với một số giá trị đầu tiên của số nguyên tố n, ta có:

$n = 2 \Rightarrow 2^2 - 1 = 3$ (nguyên tố)

$\Rightarrow N = 2.3 = 6$ (hoàn chỉnh)

$n = 3 \Rightarrow 2^3 - 1 = 7$ (nguyên tố)

$\Rightarrow N = 2^2.7 = 28$ (hoàn chỉnh)

$n = 5 \Rightarrow 2^5 - 1 = 31$ (nguyên tố)

$\Rightarrow N = 2^4.31 = 496$ (hoàn chỉnh)

$n = 7 \Rightarrow 2^7 - 1 = 127$ (nguyên tố)

$\Rightarrow N = 2^6.127 = 8128$ (hoàn chỉnh)

$n = 11 \Rightarrow 2^{11} - 1 = 2047$ (hợp số)

$n = 13 \Rightarrow 2^{13} - 1 = 8191$ (nguyên tố)

$\Rightarrow N = 2^{12}.\ 8191 = 33\ 550\ 336$ (hoàn chỉnh)

Bốn số hoàn chỉnh nhỏ nhất đã được biết từ thời thượng cổ, nhưng mãi đến thế kỉ thứ 15 người ta mới tìm thấy số hoàn chỉnh thứ năm (ứng với n = 13). Cho đến 1985, người ta đã tìm ra hơn 30 số hoàn chỉnh chẵn, số lớn nhất đã tìm được ứng với số nguyên tố n = 132 049 cho số nguyên tố Mersenne $2^{132049} - 1$ và số hoàn chỉnh $2^{132048}(2^{132049} - 1)$, gồm 79 502 chữ số trong hệ ghi thập phân. Gần đây,người ta đã tìm được số nguyên tố Mersenne $2^{216091} - 1$ cho số hoàn chỉnh $2^{216090}(2^{216091} - 1)$ gồm khoảng 140 000 chữ số trong hệ ghi thập phân.

Các nhà toán học chưa thể trả lời được rằng có hữu hạn hay vô hạn số hoàn chỉnh chẵn (có hay không có số hoàn chỉnh chẵn lớn nhất), đồng thời cũng chưa biết rằng có hay không có số hoàn chỉnh là số lẻ (chỉ biết rằng nếu có số hoàn chỉnh lẻ thì số đó phải rất lớn, lớn hơn 10^{50}).

Khái niệm về số hoàn chỉnh được *mở rộng* như sau :

Ta lấy một số tự nhiên a_1 và tính tổng của tất cả các ước số thực sự của a_1(tức là các ước số của a_1, không kể bản thân a_1), ta được a_2; tính tổng của tất cả các ước số thật sự của a_2, ta được a_3;v.v..nếu xảy ra trường hợp tổng tất cả các ước số thật sự của a_n mà cho ta a_1 thì ta được một "vòng" số sắp thứ tự $(a_1, a_2, \dots, a_n)$.

Với n = 1, ta có *số hoàn chỉnh* (tổng tất cả các ước số thật sự của a_1 bằng a_1).

Với n = 2, ta có cặp số được gọi là *cặp số bạn bè* : số này bằng tổng tất cả các ước số thật sự của số kia. Từ cổ Hi-lạp, người ta đã biết *cặp số bạn bè* nhỏ nhất là 220 và 284. Tổng tất cả các ước số thật sự của 220 là :

1 + 2 + 4 + 5 + 10 + 11 + 20 + 22 + 44 + 55 + 110 = 284, còn tổng tất cả các ước số thật sự của 284 là :

$$1 + 2 + 4 + 71 + 142 = 220.$$

Năm 1636, Fermat tìm được cặp số bạn bè khác là 17296 và 18416; và gần như đồng thời, Descartes (Đê-các) tìm ra cặp số 9363584 và 9437056. Đến thế kỉ 18, Euler công bố danh sách hơn 60 cặp số bạn bè. Điều đáng ngạc nhiên là trong thời gian khá dài,người ta cứ nghĩ rằng cặp số bạn bè nhỏ thứ hai (sau cặp số 220 và 284) là 2620 và 2924, nhưng năm 1867, một thiếu niên 16 tuổi người Y là Paganini đã tìm ra cặp số bạn bè 1180 và 1210, và đây mới đúng là cặp số bạn bè nhỏ thứ hai.Ngày nay, nhờ máy tính điện tử, người ta đã tìm ra trên 600 cặp số bạn bè. Năm 1918, người ta đã tìm ra được một "vòng" gồm 5 số là 12496, 14288, 15472, 14536 và 14264 (tổng tất cả các ước số thật sự của 12496 là 14288, tổng tất cả các ước số thật sự của 14288 là 15472,..).Nhưng cho đến nay, chưa ai tìm ra được một "vòng" gồm 3 số (hoặc chứng minh rằng không tồn tại một "vòng" như vậy).

Còn rất nhiều bài toán về số nguyên tố chưa có ai giải được. Một trong các bài toán nổi tiếng nhất là bài toán Goldbach-Euler, do hai nhà toán học Goldbach (Gon-bac, 1690-1764) và Euler (1707, 1783), đều là viện sĩ Viện Hàn lâm Peterbourg (Pê-tec-bua, Nga), đề ra năm 1742: *Mọi số chẵn lớn hơn 2 đều có thể viết dưới dạng tổng của hai số nguyên tố.*

Đây là một giả thuyết, một dự đoán, phát biểu hết sức đơn giản, ai cũng hiểu được, và có thể kiểm tra rất dễ dàng với

những số chẵn lớn hơn 2 đầu tiên:

$4 = 2 + 2$

$6 = 3 + 3$

$8 = 5 + 3$

$10 = 7 + 3 = 5 + 5$

$12 = 7 + 5$

$14 = 11 + 3 = 7 + 7$

$16 = 11 + 5 = 13 + 3$

$18 = 13 + 5 = 11 + 7$

$20 = 13 + 7 = 17 + 3$

$22 = 17 + 5 = 11 + 11$

$24 = 19 + 5 = 17 + 7$

$26 = 23 + 3 = 21 + 5$

v.v...

Người ta đã thử và thấy rằng dự đoán là đúng với mọi số chẵn > 2 và 100000. Gần 250 năm đã trôi qua, bao nhiêu nhà toán học tên tuổi đã dày công nghiên cứu, nhưng chưa ai chứng minh được rằng giả thuyết là đúng với mọi số chẵn > 2 hoặc bác bỏ giả thuyết đó (thí dụ: chỉ ra được một số chẵn lớn hơn 2 mà không thể viết được dưới dạng tổng của hai số nguyên tố). Năm 1937, viện sĩ Liên Xô Vinogradov (1891-1983) đã chứng minh được rằng: mọi số lẻ lớn hơn một số A nào đó đều có thể viết dưới dạng tổng của ba số nguyên tố; chỉ còn phải thử với tất cả những số lẻ nhỏ hơn A, là điều có thể sẽ làm được về nguyên tắc, tuy rất phức tạp, đòi hỏi rất nhiều phép tính do số A quá lớn. Kết quả mà Vinogradov đã đạt được đánh dấu một bước tiến dài trong lịch sử giải bài toán Goldbach-Euler; và điều quan trọng là phương pháp giải của Vinogradov được áp dụng để giải nhiều bài toán tổng quát của số học; vì vậy người ta coi đây là một trong những thành tựu lớn nhất của toán học hiện đại.

4 - Chứng minh định lí cơ bản của số học

Định lí- Mọi số tự nhiên lớn hơn 1 đều phân tích được ra thừa số nguyên tố một cách duy nhất (không kể thứ tự các thừa số). Số nguyên tố được coi như là một "tích" chỉ gồm mỗi một thừa số là chính nó.

Định lí trên đây, định lí cơ bản của số học, trong một thời gian rất dài được coi như là " hiển nhiên", không được nêu ra trong các cuốn sách về số học, kể từ Euclide đến Legendre (1798). Người đầu tiên phát biểu chính xác và chứng minh nó là K.Gauss (1801).

Sau đây là một cách chứng minh định lí:

∇ 1) *Mọi số lớn hơn 1 đều phân tích được ra thừa số nguyên tố.*

Dùng qui nạp toán học: Giả sử điều khẳng định là đúng với mọi số m > 1 và m < n, ta chứng minh nó đúng với n.

Nếu n là nguyên tố, thì điều đó đã rõ ràng.

Nếu n là hợp số thì theo định nghĩa, ta viết được n = a.b, với a,b < n. Theo giả thiết qui nạp, a và b là tích của các thừa số nguyên tố, do đó n cũng là tích của các thừa số nguyên tố.

2) *Mọi số lớn hơn 1 đều phân tích được ra thừa số nguyên tố một cách duy nhất.*

Cũng dùng qui nạp toán học: Giả sử mọi số m < n đều phân tích được ra thừa số nguyên tố một cách duy nhất, ta chứng minh điều đó cũng đúng với số n.

Nếu n là nguyên tố thì kết quả là hiển nhiên.

Giả sử n là hợp số và có hai cách phân tích n ra thừa số nguyên tố khác nhau:

$$n = p.q.r... = p'.q'.r'...(1)$$

trong đó p, q, r,...và p',q',r',...là các số nguyên tố và không có số nguyên tố nào cùng có mặt trong cả hai phân tích đó(vì nếu có s như vậy thì ta có thể chia cho s và có số < n mà lại có hai phân tích ra thừa số nguyên tố khác nhau, trái với giả thiết qui nạp).

Không mất tính tổng quát, có thể giả thiết p là số nguyên tố nhỏ nhất trong phân tích thứ nhất và p' là số nguyên tố nhỏ nhất trong phân tích thứ hai. Vì n là hợp số, nên $n = p^2$ và $n = p'^2$ và do $p \neq p'$ nên $p.p' < n$.

Số $m = n - pp' < n$ được phân tích ra thừa số nguyên tố một cách duy nhất (theo giả thiết qui nạp). Từ (1), ta có:

$p \mid n$ do đó $p \mid n - pp' = m$

$p' \mid n$ do đó $p' \mid n - pp' = m$

Vì vậy, phân tích m ra thừa số nguyên tố, ta có

$m = n - pp' = pp'PQ...$

với P,Q,...là số nguyên tố. Do đó

$pp' \mid n = p.q.r...$, tức $p' \mid q.r...$

Như vậy, p' là ước nguyên tố của $q.r... < n$ mà p' không trùng với một thừa số nào trong q.r...cả, điều này trái với giả thiết qui nạp là mọi số nhỏ hơn n đều phân tích được ra thừa số nguyên tố một cách duy nhất. □

Bài tập

2.1 - Chứng minh rằng: a) mọi số nguyên tố lớn hơn 2 đều có dạng $4n \pm 1$ (n > 0; b) mọi số nguyên tố lớn hơn 3 đều có dạng $6n \pm 1$ (n > 0).

2.2 - Nếu p là số nguyên tố > 3 thì $p^2 - 1$ chia hết cho bao nhiêu? Nếu p và q là các số nguyên tố > 3 thì $p^2 - q^2$ chia hết cho bao nhiêu?

2.3 - Cho p là số nguyên tố và một trong hai số $8p + 1$ và $8p - 1$ là số nguyên tố; số thứ ba là nguyên tố hay hợp số?

2.4- a) Nếu $p(\geq 5)$ và $2p + 1$ là các số nguyên tố thì $4p + 1$ là số nguyên tố hay hợp số?

b) Nếu p và $8p^2 + 1$ là các số nguyên tố thì $8p^2 - 1$ và $8p^2 + 2p + 1$ là các số nguyên tố hay hợp số ?

2.5- Tìm số nguyên tố p sao cho :

a) $2p + 1$ là lập phương của một số tự nhiên;

b) $13p + 1$ là lập phương của một số tự nhiên.

2.6- Hai số $2^n + 1$ và $2^n - 1$ ($n > 2$) có thể đồng thời là số nguyên tố hay đồng thời là hợp số được không ?

2.7- Tìm số nguyên tố p sao cho:

a) $p + 10$ và $p + 14$ cũng là số nguyên tố;

b) $p + 2$, $p + 6$ và $p + 8$ cũng là các số nguyên tố;

c) $p + 6$, $p + 8$, $p + 12$ và $p + 14$ cũng là các số nguyên tố

2.8 - Chứng minh rằng số dư trong phép chia một số nguyên tố p cho 30 chỉ có thể là 1 hoặc là một số nguyên tố

Nếu chia p cho 60 thì sao?

2.9 - Tìm k để cho trong 10 số liên tiếp:

$k + 1, k + 2, \ldots, k + 10$

có nhiều số nguyên tố nhất.

2.10 - Các số 3, 5, 7 là ba số lẻ liên tiếp và đều là số nguyên tố. Hãy tìm tất cả các bộ ba số lẻ liên tiếp và đều là số nguyên tố.

2.11 - Ta gọi p và q là hai số nguyên tố liên tiếp nếu giữa p và q không có một số nguyên tố nào; thí dụ: 7 và 11.

Tìm ba số nguyên tố liên tiếp p, q, r sao cho $p^2 + q^2 + r^2$ cũng là số nguyên tố.

2.12 - Tìm số nguyên tố p sao cho p vừa là tổng của hai số nguyên tố, vừa là hiệu của hai số nguyên tố.

2.13 - Tìm tất cả các số n để cho:

a) $n^4 + 4$ là số nguyên tố;

b) $n^4 + n^2 + 1$ là số nguyên tố;

c) $n^3 - n^2 + n + 1$ là số nguyên tố.

2.14 - Tìm tất cả các số nguyên tố p:

a) p có dạng $\frac{n(n+1)}{2} - 1$ ($n \geq 1$);

b) p có dạng $\frac{n(n+1)(n+2)}{6} + 1$ ($n \geq 1$).

2.15 - Chứng minh rằng có vô số giá trị của n sao cho mọi số có dạng $m^4 + n$ đều là hợp số.

2.16 - Chứng minh rằng nếu (n - 1)! chia hết cho n thì n không phải là số nguyên tố.(Thí dụ: 5! = 120 chia hết cho 6).

2.17 - Cho N là tích của tất cả các/số nguyên tố p:

/số nguyên tố không lớn hơn

N = 2.3.5....p.

Chứng minh rằng N - 1 và N + 1 đều không thể là số chính phương.

2.18 - a) Chứng minh rằng có duy nhất một số nguyên tố có dạng $x^3 + 1$.

b) Tìm ba số nguyên tố có dạng $x^3 + 2$.

2.19 - Chứng minh rằng có vô số số nguyên tố:

a) có dạng 4x + 3;

b) có dạng 6x + 5.

2.20 - Chứng minh rằng từ giả thuyết Goldbach-Euler suy ra được: mọi số lẻ > 7 đều có thể viết dưới dạng tổng của ba số nguyên tố lẻ.

CHƯƠNG 3

PHƯƠNG TRÌNH DIOPHANTE

Có bài toán dân gian sau đây:

Trăm trâu trăm cỏ,

Trâu đứng ăn năm,

Trâu nằm ăn ba,

Lụ khụ trâu già,

Ba con một bó.

Hỏi có bao nhiêu trâu đứng, bao nhiêu trâu nằm, bao nhiêu trâu già ?

Gọi số trâu đứng là x,

số trâu nằm là y

thì số trâu già là $100 - (x + y)$.

Ta có phương trình:

$$5x + 3y + \frac{100 - (x + y)}{3} = 100$$

hay $7x + 4y = 100$

Nếu không có điều hạn chế gì thì phương trình này rất dễ giải; nó có vô số nghiệm:

$$\begin{cases} x \text{ tùy ý} \\ y = \dfrac{100 - 7x}{4} \end{cases}$$

Nhưng theo đề toán thì x, y (số trâu) phải là số nguyên (dương), nên ta phải tìm nghiệm nguyên (dương) của phương trình.

Đây là một thí dụ về *phương trình Diophante (Điôphan).*

Một phương trình có nhiều ẩn số, với tất cả các hệ số đều là số nguyên, và ta phải tìm nghiệm nguyên của nó, được gọi là một phương trình Diophante.

Phương trình Diophante nói chung là có nhiều nghiệm nguyên, vì vậy người ta cũng gọi đó là *phương trình vô định.*

Thí dụ: $7x + 4y = 100$

$$x^2 + y^2 = z^2$$

$$x^3 - 7y^2 = 1.$$

Phương trình mang tên nhà toán học cổ Hi Lạp là Diophante (thế kỉ thứ 3), tác giả cuốn sách "Số học" đã có tác dụng rất lớn đến sự phát triển của toán học.

Phương trình Diophante là một lĩnh vực rất lí thú và rất khó của toán học, trong đó chúng ta tìm thấy đóng góp của rất nhiều nhà toán học nổi tiếng: Euclide và Archimède, Fermat, Euler và Lagrange, Gauss, Dirichlet, Riemann và Hilbert,v.v...

Sau đây, chúng ta sẽ xét một vài phương trình Diophante đơn giản nhất.

■ 1- Phương trình bậc nhất

1.1- Phương trình bậc nhất hai ẩn

Phương trình bậc nhất hai ẩn là phương trình có dạng

$$ax + by = c$$

trong đó a, b, c là số nguyên, với $a \neq 0$ *và* $b \neq 0$.

Nếu a, b, c có ước chung lớn nhất là d $\neq$ 1 thì ta có thể chia hai vế cho d, để được phương trình đơn giản hơn. Thí dụ:

$$6x + 4y = 14 \Leftrightarrow 3x + 2y = 7$$

$$12x + 6y = 15 \Leftrightarrow 4x + 2y = 5$$

Vì vậy, có thể giả thiết *các hệ số a, b, c không có ước chung nào $\neq 1$*, tức là *nguyên tố cùng nhau.*

Có thể chứng minh được hai định lí sau:

Định lí 1- *Phương trình $ax + by = c$ có nghiệm nguyên khi và chỉ khi $(a,b) = 1$ (a, b nguyên tố cùng nhau).*

Thí dụ:

$7x + 4y = 100$ có nghiệm nguyên vì $(7,4) = 1$.

$4x + 2y = 5$ không có nghiệm nguyên vì $(4,2) = 2$.

Định lí 2- *Nếu phương trình $ax + by = c$ có một nghiệm nguyên là cặp số $(x_0;y_0)$ thì nó có vô số nghiệm nguyên, đó là tập hợp tất cả các cặp số $(x;y)$ có dạng*

$$\begin{cases} x = x_0 + bt \\ y = y_0 - at \end{cases}$$

với t là số nguyên tùy ý ($t = 0, \pm 1, \pm 2, \ldots$)

Ta gọi $(x_0; y_0)$ là *một nghiệm riêng* của phương trình, còn công thức trên đây của x,y cho ta *nghiệm tổng quát* của phương trình (ta cũng nói đó là *công thức tổng quát của nghiệm*).

Do định lí 2, muốn giải phương trình $ax + by = c$, với $(a,b) = 1$, ta chỉ cần tìm một nghiệm riêng nào đó của nó.

Thí dụ: Giải phương trình

$$7x + 4y = 100.$$

Ta thấy ngay được rằng phương trình có một nghiệm riêng là $(x = 0; y = 25)$, do đó có nghiệm tổng quát là

$$x = 0 + 4t$$

$$y = 25 - 7t \quad (t = 0, \pm 1, \pm 2...)$$

Đối với bài toán "trăm trâu, trăm cỏ", ta phải tiếp tục xét thêm: x, y (số trâu) phải là số dương, tức

$$x = 4t > 0, \Leftrightarrow \quad t > 0$$

$$y = 25 - 7t > 0 \quad t < 4$$

nghĩa là chỉ được lấy $t = 1,2,3$:

$$t = 1 \Rightarrow x = 4; y = 18; z = 78$$

$$t = 2 \Rightarrow x = 8; y = 11; z = 81$$

$$t = 3 \Rightarrow x = 12; y = 4; z = 84$$

Chứng minh định lí 2 (ta thừa nhận định lí 1):

∇ Cho phương trình

$$ax + by = c \ (1)$$

có một nghiệm là $(x_0; y_0)$; như vậy theo định lí 1, ta có $(a,b) = 1$.

1) Mọi cặp số $(x_0 + bt; y_0 - at)$ đều là nghiệm của (1).

Thực vậy, ta có

$$a(x_0 + bt) + b(y_0 - at) = ax_0 + abt + by_0 - bat = ax_0 + by_0.$$

Theo giả thiết, $ax_0 + by_0 = c$, do đó

$$a(x_0 + bt) + b(y_0 - at) = c,$$

chứng tỏ $(x_0 + bt; y_0 - at)$ là nghiệm của (1).

2) Mọi nghiệm $(x_1; y_1)$ của (1) đều có dạng

$$x_1 = x_0 + bt$$

$$y_1 = y_0 - at$$

Thực vậy, vì $(x_0; y_0)$ và $(x_1; y_1)$ là hai nghiệm của phương trình nên

$$ax_0 + by_0 = c$$

$$ax_1 + by_1 = c$$

do đó $\quad a(x_1 - x_0) = b(y_0 - y_1)$ (2)

chứng tỏ $\quad a(x_1 - x_0) \vdots b.$

mà $(a,b) = 1$ nên $x_1 - x_0 \vdots b$, nghĩa là có một số nguyên t sao cho

$$x_1 - x_0 = bt \text{ hay } x_1 = x_0 + bt.$$

Thay vào (2), có

$$abt = b(y_0 - y_1) \text{ hay } y_1 = y_0 - at$$ □

Chú ý rằng *nghiệm tổng quát của phương trình* $ax + by = c$ cũng có thể viết dưới dạng

$$x = x_0 - bt$$

$$y = y_0 + at$$

1.2- Phương pháp tìm một nghiệm riêng của phương trình $ax + by = c$

Phương pháp sau đây dựa vào một định lí về liên phân số (bạn đọc có thể xem chứng minh ở phần phụ lục), giúp tìm ra dễ dàng một nghiệm riêng của $ax + by = c$.

Thí dụ 1- Giải phương trình

$$40x + 31y = 1.$$

∇ Vì $(40,31) = 1$, nên phương trình có nghiệm nguyên. Ta tìm một nghiệm riêng theo các bước sau đây:

Bước 1. Viết thuật toán Euclide để tìm UCLN của 40 và 31:

$$40 = 31.1 + 9$$

$$31 = 9.3 + 4$$

$$9 = 4.2 + 1$$

Vì (40,31) = 1, nên quá trình kết thúc với số dư là 1.

Bước 2. Để viết được số 1 dưới dạng $40x_0 + 31y_0$, ta viết các đẳng thức trên đây từ dưới lên trên, đưa số dư về vế trái:

$$1 = 9 - 4.2 \text{ (a)}$$

$$4 = 31 - 9.3 \text{ (b)}$$

$$9 = 40 - 31.1 \text{ (c)}$$

Thay giá trị của số 4 từ (b) vào (a):

$$1 = 9 - (31 - 9.3).2 = -31.2 + 9.7$$

Thay giá trị của số 9 từ (c) vào đây, được:

$$1 = -31.2 + (40 - 31).7 = 40.7 - 31.9 = 40.7 + 31.(-9).$$

Bước 3. Từ đẳng thức trên, có $x_0 = 7$, $y_0 = -9$ và phương trình đã cho có nghiệm là

$$x = 7 - 31t$$

$$y = -9 + 40t,\ t \in Z.$$ □

Việc tính toán ở bước 2 có thể thay thế bằng một thuật toán đơn giản hơn như sau:

Bước 2. Lấy thương trong dãy các phép chia ở bước 1, đó là: 1,3,2 rồi tính phân số

$$m = 1 + \cfrac{1}{3 + \cfrac{1}{2}}$$

được $m = \frac{9}{7}$

Bước 3. Giá trị tuyệt đối của một nghiệm riêng là

$$|x_0| = 7$$

$$|y_0| = 9$$

(vì $|a| > |b|$ nên ta lấy $|x_0| < |y_0|$)

Bước 4. Thử để xác định dấu của x_0 và y_0.

$$40.7 = 280$$

$$31.9 = 279$$

Do đó: $40.7 - 31.9 = 1$ hay $40.7 + 31(-9) = 1$.

Vậy $x_0 = 7$

$y_0 = -9$

Nghiệm tổng quát của phương trình đã cho là

$$x = 7 + 31t$$

$$y = -9 - 40t \quad (t \in Z)$$

Thí dụ 2 - Giải phương trình

$$7x - 11y = 15$$

∇ Phương trình này có nghiệm nguyên vì $(7, 11) = 1$.

Trước hết, chú ý rằng nếu $(x_0; y_0)$ là một nghiệm riêng của phương trình

$$ax + by = 1$$

thì $(cx_0; cy_0)$ là một nghiệm riêng của phương trình

$$ax + by = c$$

bởi vì từ $\quad ax_0 + by_0 = 1$

suy ra được $\quad a(cx_0) + b(cy_0) = c.$

Do đó, trước hết ta tìm một nghiệm riêng của phương trình

$$7x - 11y = 1$$

Bước 1. Viết thuật toán Euclide để tìm (11, 7):

$$11 = 7.1 + 4$$

$$7 = 4.1 + 3$$

$$4 = 3.1 + 1$$

Bước 2.

$$m = 1 + \frac{1}{1 + \frac{1}{1}} = \frac{3}{2}$$

Bước 3.

$$| x_0 | = 3$$

$$| y_0 | = 2$$

(vì $|a| < |b|$ nên phải lấy $|x_0| > |y_0|$).

Bước 4.

$7.3 = 21$, $11.2 = 22$, do đó

$-21 + 22 = 1$ hay $7.(-3) - 11(-2) = 1$.

Vậy $x_0 = -3$

$y_0 = -2$

Suy ra một nghiệm riêng của phương trình:

$$7x - 11y = 15$$

là $x_0 = -3.15 = -45$

$y_0 = -2.15 = -30.$

và nghiệm tổng quát là

$$x = -45 + 11t$$

$$y = -30 - 7t \ (t \in Z)$$ □

1.3 - Phương trình bậc nhất n ẩn (n > 2)

Người ta chứng minh được rằng một phương trình bậc nhất *n* ẩn (sau khi chia cả hai vế của phương trình cho UCLN của các hệ số của nó) có nghiệm nguyên khi và chỉ khi *các hệ số của các ẩn là các số nguyên tố cùng nhau.*

Thí dụ 1. Giải phương trình

$$2x - 5y - 6z = 4$$

∇ Phương trình này có nghiệm nguyên vì $(2,5,6) = 1$.

Ta thấy: phương trình có hai hệ số (của hai ẩn) là nguyên tố cùng nhau: $(2,5) = 1$, vì vậy ta đưa phương trình về dạng

$$2x - 5y = 4 + 6z.$$

Lấy $z = u$ là số nguyên tùy ý và đặt

$$4 + 6z = 4 + 6u = c$$

ta có $2x - 5y = c$.

Phương trình này có một nghiệm riêng là

$$x_0 = 3c$$

$$y_0 = c$$

do đó có nghiệm tổng quát là

$$x = 3c + 5t$$

$$y = c + 2t \ (t \in \mathbb{Z})$$

Thay $c = 4 + 6u$ vào, ta được nghiệm tổng quát của phương trình $2x - 5y - 6z = 4$ là:

$$x = 3(4 + 6u) + 5t = 12 + 18u + 5t$$

$$y = 4 + 6u + 2t$$

$$z = u$$

trong đó u,t là những số nguyên tùy ý. □

Thí dụ 2. Giải phương trình

$$6x + y + 3z = 15.$$

∇ Phương trình này *có hệ số của một ẩn (y) bằng 1*. Ta thấy x,z có thể lấy bất kì giá trị nguyên nào, lúc đó ta cũng có một giá trị nguyên của y. Phương trình có nghiệm tổng quát là

$y = 15 - 6u - 3t$

$x = u$

$z = t$

trong đó u và t là những số nguyên tùy ý. ❒

Thí dụ 3. Giải phương trình

$$6x + 15y + 10z = 3.$$

∇ Phương trình có nghiệm nguyên vì $(6,15,10) = 1$.

Ta tìm cách biến đổi và đặt ẩn phụ để đưa về phương trình *có hệ số của một ẩn là bằng 1:*

$$6x + 10(y + z) + 5y = 3$$

Đặt $y + z = u \Rightarrow 6x + 10u + 5y = 3$

$$x + 10u + 5(x + y) = 3$$

Đặt $x + y = v, \Rightarrow x + 10u + 5v = 3$

Nghiệm tổng quát của phương trình đã cho là

$x = 3 - 10u - 5v$

$y = -3 + 10u + 4v \qquad (y = v - x)$

$z = 3 - 9u - 6v \qquad (z = u - y = u - v + x)$

trong đó u,v là các số nguyên tùy ý. ❒

Chú ý rằng ta cũng có thể biến đổi và đặt ẩn phụ để đưa về phương trình *có hai hệ số (của hai ẩn) là nguyên tố cùng nhau:*

$$6x + 15y + 10z = 3$$

$$6(x + z) + 15y + 4z = 3$$

Đặt $x + z = u \Rightarrow 6u + 15y + 4z = 3$

Ta có $(15,4) = 1$, vì vậy ta viết

$$15y + 4z = 3 - 6u$$

Đặt $3 - 6u = c \Rightarrow 15y + 4z = c$.

Tiếp tục giải như trong thí dụ 1.

1.4 - Giải hệ phương trình bậc nhất

Bài toán. Tìm một số nguyên, biết rằng khi chia số đó cho 3, cho 5 và cho 7 thì có số dư tương ứng là 2, 3 và 4.

∇ Gọi số phải tìm là x.

Chia x cho 3, dư 2, vậy x có dạng $3u + 2$ (u là số nguyên).

Tương tự, x có dạng $5y + 3$, $7z + 4$ (y,z là số nguyên).

Ta có

$$x = 3u + 2 = 5y + 3 = 7z + 4$$

Ta phải giải hệ phương trình

$$\begin{cases} 3u + 2 = 5y + 3 & (1) \\ 5y + 3 = 7z + 4 & (2) \end{cases}$$

$$(1) \Leftrightarrow 3u - 5y = 1 \Leftrightarrow u = 2 + 5v \quad (3)$$

$$y = 1 + 3v \quad (4) \quad (v \in \mathbb{Z})$$

Thay biểu thức của y từ (4) vào (2), được

$$5\,(1 + 3v) = 7z + 4$$

$$15v - 7z = -4$$

Giải phương trình này, được

$$v = -4 + 7t \quad (5)$$

$$z = -8 + 15t \quad (t \in \mathbb{Z})$$

Thay giá trị của v từ (5) vào (3):

$$u = 2 + 5\,(-4 + 7t) = -18 + 35t$$

Do đó:

$$x = 3u + 2 = -52 + 105t \quad (t \in \mathbb{Z})$$ □

Thí dụ: $x = -52$ (với $t = 0$), 53 (với $t = 1$), 158 (với $t = 2$), 263 (với $t = 3$), -157 (với $t = -1$), -262 (với $t = -2$),v.v...

Chú ý rằng bài toán trên đây chính là bài toán "Hàn Tín điểm binh", nếu yêu cầu nghiệm phải nguyên dương (xem chương I). Có thể thấy rằng phương trình đồng dư

$$x = 2 \pmod 3$$

cũng chính là phương trình Diophante

$$x = 2 + 3u$$

trong đó ta chỉ quan tâm đến ẩn x.

Nếu x phải nguyên dương thì trong công thức tìm được trên đây ta phải viết

$$x = -52 + 105t \ (t \geq 1)$$

Công thức này trùng với công thức đã tìm thấy ở lời giải bài toán " Hàn Tín điểm binh":

$$x = 53 + 105t \ (t \geq 0).$$

Bài tập

3.1 - Giải các phương trình

a) $5x + 3y = 2$; b) $32x - 40y = 38$;

c) $38x + 117y = 15$; d) $21x - 17y = -3$.

3.2 - Với giá trị nguyên nào của x thì $\frac{5x + 2}{17}$ là một số nguyên?

3.3 - Tìm số tự nhiên chia hết cho 7 và khi chia cho 2, 3, 4, 5, 6 luôn cho số dư là 1.

3.4 - Tìm năm sinh của nhà thơ Nguyễn Du, biết rằng năm 1786 thì tuổi của ông bằng tổng các chữ số của năm ông sinh ra.

3.5 - Một bài toán dân gian:

Ba người đi câu được một số cá. Trời đã tối và mệt lả, họ vứt cá trên bờ sông, rồi mỗi người tìm một nơi lăn ra ngủ. Người thứ nhất thức dậy, đến bờ sông, đếm số cá thấy chia ba thừa một con, bèn vứt bớt 1 xuống sông và xách 1/3 về nhà. Người thứ hai thức dậy,

tưởng hai bạn mình còn ngủ, đến bờ sông, đếm số cá, vứt 1 xuống sông và xách 1/3 về nhà. Người thứ ba thức dậy, cứ nghĩ là mình dậy sớm nhất, đến bờ sông, đếm số cá xong vứt 1 con, và xách 1/3 về nhà.

Cho biết họ là ba chàng đi câu tồi, bạn hãy tính xem họ câu được bao nhiêu cá?

3.6 - Giải và biện luận theo số nguyên m các phương trình:

a) $6x - 11y = m + 2$; b) $15x + 25y = 2m - 1$;

c) $3x - (m - 2)y = m + 1$; d) $5x + (3m + 1)y = 2m + 1$.

3.7 - Cho phương trình $ax + by = c$, trong đó a,b,c là các số tự nhiên $\neq 0$ và $(a,b) = 1$. Chứng minh rằng phương trình không có nghiệm tự nhiên nếu $c = ab$.

3.8 - Chứng minh rằng với mỗi cặp số nguyên dương m,n cho trước, có một phương trình bậc nhất hai ẩn $ax + by = c$ với hệ số a,b,c là những số nguyên, nhận $x = m$, $y = n$ là nghiệm nguyên dương duy nhất.

3.9 - Chứng minh rằng với mỗi số nguyên dương m cho trước bao giờ cũng có một phương trình vô định bậc nhất hai ẩn $ax + by = c$ có đúng m nghiệm nguyên dương.

3.10 - Giải các phương trình:

a) $2x + 3y + 5z = 15$; b) $23x - 53y + 80z = 101$;

c) $6x + 15y + 6z - 10t = 13$; d) $8x + 15y - 6z - 20t = 21$.

3.11- Giải các hệ phương trình:

a) $3x + 2y = 1$
$3x + 6y + 2z = -1$

b) $2x - 3y = 1$
$3x - 2y + 3z = 5$

c) $x + 4y + 2z = 7$
$2x - 7y - 5z = -7$

d) $3x - 5y - 3z = 1$
$2x - 3y + 3z = -3$

3.12 - Giải và biện luận theo số nguyên m:

a) $3x + 2y = 1$
$3x + 6y + (m + 1)z = m - 2$

b) $3x - 5y - 3z = 1$

$2x - 3y + (m - 2)z = 1 - m$

3.13 - Tìm tất cả các số tự nhiên x sao cho:

a) x chia hết cho 9 và $x + 1$ chia hết cho 25;

b) x chia hết cho 21 và $x + 1$ chia hết cho 165;

c) x chia hết cho 9, $x + 1$ chia hết cho 25 và $x + 2$ chia hết cho 4.

3.14 - Tìm tất cả các số nguyên mà khi chia chúng cho 19 và 11 thì số dư tương ứng là 4 và 1.

3.15 - Tìm tất cả các số nguyên x sao cho $\frac{3x - 1}{7}$ và $\frac{7x - 1}{5}$ là những số nguyên.

3.16 - Tìm tất cả các số nguyên x và y sao cho cả hai số $3x - y + 1$ và $2x + 3y - 1$ đều chia hết cho 7.

3.17 - Trong các số tự nhiên từ 200 đến 500, những số nào chia cho 4, 5, 7 có dư lần lượt là 3, 4, 5 ?

3.18 - Tìm số tự nhiên nhỏ nhất sao cho khi chia nó cho 7, 5, 3, 11 ta được số dư tương ứng là 3, 2, 1, 9.

3.19 - Một bài toán dân gian:

"Mai em đi chợ phiên,
Anh gửi một tiền,
Mua cam cùng quít.
Không nhiều thì ít
Mua lấy một trăm.
Cam ba đồng một,
Quít một đồng năm,
Thanh yên tươi tốt
Năm đồng một trái."

Hỏi mua mỗi thứ mấy trái ? (Biết rằng: một tiền gồm 60 đồng).

3.20 - a) Trên đường thẳng $8x - 13y + 6 = 0$ hãy tìm các điểm nguyên (tức là có tọa độ là số nguyên) nằm giữa hai đường thẳng $x = -10, x = 50$.

b) Chứng minh rằng trong hình chữ nhật giới hạn bởi các đường thẳng $x = 6, x = 42, y = 2, y = 17$ không có điểm nguyên nào thuộc đường thẳng $3x + 5y = 7$.

■ 2 - Phương trình $x^2 + y^2 = z^2$ và định lí lớn Fermat

2.1 - Chúng ta đã biết định lí Pythagore (Pitago): trong một tam giác vuông có cạnh huyền là c, hai cạnh góc vuông là a, b, ta có:

$$a^2 + b^2 = c^2.$$

Có trường hợp a, b, c đều là số nguyên dương, thí dụ:

$$3^2 + 4^2 = 5^2$$

Từ thời xa xưa, người ta đã đi tìm những bộ ba số nguyên dương x, y, z như vậy, được gọi là các số Pythagore, thỏa mãn phương trình:

$$x^2 + y^2 = z^2 \quad (1)$$

Thực ra, từ trước Pythagore cả nghìn năm, vào khoảng 2000 năm trước Công nguyên, những người Babilon đã thấy rằng bộ ba số:

$$x = p^2 - q^2$$

$$y = 2pq$$

$$z = p^2 + q^2$$

trong đó p, q là các số nguyên dương bất kì với $p > q$, là các số thỏa mãn (1):

$$(p^2 - q^2)^2 + (2pq)^2 = (p^2 + q^2)^2.$$

Thí dụ: Với $p = 2$, $q = 1$ có

$$x = 3, y = 4, z = 5 \ (3^2 + 4^2 = 5^2)$$

Với $p = 3, q = 1$ có

$x = 8, y = 6, z = 10$ $(8^2 + 6^2 = 10^2)$

Với $p = 3, q = 2$ có

$x = 5, y = 12, z = 13$ $(5^2 + 12^2 = 13^2$

Bây giờ ta đi tìm nghiệm tổng quát của phương trình (1).

Chia hai vế của (1) cho z^2 được:

$$\frac{x^2}{z^2} + \frac{y^2}{z^2} = 1$$

Đặt $\frac{x}{z} = X, \frac{y}{z} = Y$, có phương trình:

$$X^2 + Y^2 = 1 \quad (2)$$

với X,Y là các số hữu tỉ

$$(2) \Leftrightarrow Y^2 = 1 - X^2$$

$$Y^2 = (1 - X)(1 + X)$$

Giả sử $X \neq -1$, ta chia hai vế cho $(1 + X)^2$:

$$\left(\frac{Y}{1 + X}\right)^2 = \frac{1 - X}{1 + X}$$

Đặt $t = \frac{Y}{1 + X}$, ta được:

$$t^2 = \frac{1 - X}{1 + X}$$

từ đó suy ra $X = \frac{1 - t^2}{1 + t^2}$, $Y = \frac{2t}{1 + t^2}$ (3)

Với mọi giá trị hữu tỉ của t, ta có các giá trị hữu tỉ của X và Y thỏa mãn (2). Ngược lại, mỗi nghiệm hữu tỉ của (2) đều có dạng (3) (trừ trường hợp $X = -1, Y = 0$). Như vậy,

(3) là công thức của nghiệm tổng quát của (2).

Từ (3), ta có công thức của *nghiệm nguyên tổng quát* của (1), bằng cách đặt $t = \frac{p}{q}$ với $(p,q) = 1$. Lúc đó ta có:

$$X = \frac{x}{z} = \frac{p^2 - q^2}{p^2 + q^2} \quad (4)$$

$$Y = \frac{y}{z} = \frac{2pq}{p^2 + q^2}$$

Từ đây, thấy ngay rằng các số nguyên sau đây thỏa mãn phương trình (1):

$$\begin{cases} x = m(p^2 - q^2) \\ y = m.2pq \\ z = m(p^2 + q^2 \quad (5) \end{cases}$$

với m nguyên bất kì.

Nếu các số $p^2 - q^2$, 2pq và $p^2 + q^2$ có ước chung $d > 1$ thì có thể chia chúng cho d và ta có một nghiệm nguyên mới của (1), khác với nghiệm (5). Nhưng điều này không thể xảy ra, do đó (5) cho nghiệm tổng quát của (1).

Thực vậy, vì $(p,q) = 1$ nên chỉ có thể là: p và q chẵn lẻ khác nhau hoặc cả hai cùng lẻ.

- Trong trường hợp p,q chẵn lẻ khác nhau thì $p^2 - q^2$, 2pq và $p^2 + q^2$ không thể có ước chung $d > 1$, vì nếu có số d như vậy thì d phải lẻ (do $p^2 - q^2$ lẻ) và d phải là ước của $(p^2 - q^2) + (p^2 + q^2) = 2p^2$ (do d lẻ nên d là ước của p) và của $(p^2 + q^2) - (p^2 - q^2) = 2q^2$ (d cũng là ước của q), trái với giả thiết $(p,q) = 1$.

Trong trường hợp p,q cùng lẻ, ta đặt $p + q = 2P$ và $p - q = 2Q$ và có $(P,Q) = 1$ và P, Q chẵn lẻ khác nhau (vì P + Q lẻ). Thay vào (4), được:

$$\frac{x}{z} = \frac{2PQ}{P^2 + Q^2}, \qquad \frac{y}{z} = \frac{P^2 - Q^2}{P^2 + Q^2}$$

nghĩa là ta có kết quả tương tự như (4), chỉ khác là x và y đổi chỗ cho nhau, và thay vì p,q thì có P,Q với $(P,Q) = 1$ và P, Q chẵn lẻ khác nhau.

Như vậy, công thức (5) cho nghiệm tổng quát của (1).

Dịnh lí- *Nghiệm nguyên tổng quát của phương trình*

$$x^2 + y^2 = z^2$$

là

$$\begin{cases} x = m(p^2 - q^2) \\ y = 2mpq \\ z = m(p^2 + q^2) \end{cases}$$

trong đó m, p, q là các số nguyên bất kì với $(p,q) = 1$, và p, q chẵn lẻ khác nhau (trong công thức của nghiệm, x và y có thể đổi chỗ cho nhau).

Dịnh lí này đã được biết từ Euclide.

Với $m = 1$, các giá trị của x, y, z nguyên tố cùng nhau.

Cho p, q một số giá trị, ta có các *bộ ba số Pythagore:*

(3; 4; 5), (5; 12; 13), (8; 15; 17), (7; 24; 25), (21; 20; 29), (9; 40; 41),...

2.2 - Định lí lớn Fermat

Chúng ta đã thấy rằng phương trình

$$x^2 + y^2 = z^2$$

có vô số nghiệm nguyên. Thế nhưng các phương trình

$$x^3 + y^3 = z^3$$

$$x^4 + y^4 = z^4$$

đều không có nghiệm nguyên. Vào khoảng năm 1630, nhà toán học Pháp Fermat đã viết bên lề cuốn sách về các số Pythagore như sau:

" Ngược lại, không thể phân tích một lập phương thành tổng của hai lập phương; cũng như một lũy thừa bậc 4 thành tổng của hai lũy thừa bậc 4...và một cách tổng quát, không thể phân tích một lũy thừa với số mũ lớn hơn 2 thành tổng của hai lũy thừa với cùng số mũ đó. Tôi đã phát minh ra chân lí này bằng một chứng minh tuyệt diệu, nhưng lề sách này quá chật nên không thể ghi lại được".

Như vậy Fermat đã nêu lên (và khẳng định mình đã chứng minh được) rằng:

Với mọi số tự nhiên $n > 2$, phương trình

$$x^n + y^n = z^n$$

không có nghiệm nguyên dương.

Mệnh đề này được gọi là *bài toán Fermat hay định lí lớn Fermat* (còn định lí: "Với p nguyên tố thì $n^p - n$ chia hết cho n" được gọi là định lí nhỏ Fermat). Đã hơn 300 năm nay, bài toán Fermat là một trong những sự kiện lí thú nhất trong lịch sử toán học.

Fermat không để lại chứng minh của định lí. Người ta chỉ tìm thấy trong giấy tờ của Fermat phần chứng minh với $n = 4$. Bao nhiêu nhà toán học lừng danh đã đi vào vấn đề này và chỉ đạt được kết quả trong một số trường hợp riêng lẻ: Euler đã chứng minh cho $n = 3$ (năm 1770), A. Legendre (Lơ-giăng, người Pháp, 1752-1833) và Dirichlet chứng minh cho $n = 5$ (năm 1825). Dễ thấy rằng trường hợp $n = 6$ qui về n

= 3 và một cách tổng quát, chỉ cần chứng minh định lí cho số mũ n nguyên tố. Năm 1839, nhà toán học Pháp G. Lamé (Lamê, 1795-1870) đã chứng minh được cho n = 7.

Kết quả đáng kể là của nhà toán học Đức E. Kummer (Cumơ, 1810-1893) đã chứng minh được rằng định lí đúng với mọi $n \leq 100$. Sau đó, nhờ máy tính điện tử, người ta đã kiểm tra được định lí với mọi số nguyên tố nhỏ hơn 100 000 (cho đến năm 1985). Nhà toán học trẻ Hà Lan G. Faltings (sinh năm 1954) đã có đóng góp mới cho định lí Fermat với việc chứng minh (năm 1983) rằng phương trình $x^n + y^n = z^n$ với $n > 3$, nếu có nghiệm nguyên thì chỉ có một số hữu hạn nghiệm mà thôi.

Điều có ý nghĩa đối với sự phát triển của toán học là trong khi đi tìm chứng minh của định lí, các nhà toán học đã sáng tạo ra những lí thuyết toán học mới , những phương pháp mới mà thời Fermat chưa được biết tới. Đáng lưu ý là đã có nhiều "chứng minh" được công bố, và sau đó được phát hiện là sai lầm (gần đây nhất là "chứng minh" năm 1988 của Miyaoka ở CHLB Đức).

Vì vậy, người ta không khỏi dè dặt đón nhận tin A. Wiles ở trường đại học Cambridge (Anh) công bố vào ngày 23-6-1993 bản chứng minh của định lí Fermat (dài khoảng 200 trang!). Quả thật, chỉ một thời gian ngắn sau đó, nhiều nhà toán học và cả Wiles đã phát hiện một thiếu sót trong chứng minh này. Và A. Wiles đã cùng với học trò của mình là R.Taylor nhanh chóng sửa chữa được thiếu sót đó, qua bài báo được công bố ngày 7-10 - 1994. Như vậy, A. Wiles (cùng với R. Taylor) đã có vinh dự lớn kết thúc một cuộc hành trình dài 3 thế kỉ đi tìm lời giải của một trong những bài toán khó nhất và hấp dẫn nhất từ xưa đến nay.

= 3 - Một số phương trình bậc hai và cao hơn

3.1 -Không có một phương pháp chung nào để giải được mọi phương trình Diophante bậc 2 và cao hơn. Đối với mỗi phương trình, ta phải xem xét đặc điểm của nó để tùy trường hợp cụ thể, có thể phân tích ra thừa số hoặc viết dưới dạng tổng rồi vận dụng các tính chất chia hết; có thể thử để thấy một nghiệm (trong trường hợp dễ thấy) rồi từ đó tìm cách suy ra các nghiệm khác hoặc chứng minh rằng phương trình không thể có nghiệm nào khác...

Thí dụ 1- Tìm nghiệm tự nhiên của phương trình

$$2x^3 + xy = 7.$$

∇ Ta có phương trình tương đương:

$$x.(2x^2 + y) = 7$$

Vì 7 là số nguyên tố, nên phải có

$$x = 1 \qquad \text{hoặc} \qquad x = 7$$

$$2x^2 + y = 7 \qquad\qquad 2x^2 + y = 1$$

Với $x = 1$ thì $y = 7 - 2x^2 = 5$

$x = 7$ thì $y = 1 - 2x^2 < 0.$

Vậy ta có nghiệm duy nhất là (1; 5). □

Thí dụ 2- Giải phương trình (tìm nghiệm nguyên):

∇ $$6x^2 + 5y^2 = 74.$$

Phương trình phải giải tương đương với:

$$6\,(x^2 - 4) = 5\,(10 - y^2)$$

Vì (5,6) = 1, nên phải có:

$x^2 - 4 \,\vdots\, 5$ tức $x^2 - 4 = 5u$

$10 - y^2 \,\vdots\, 6$ tức $10 - y^2 = 6v$

và $6.5u = 5.6v$, do đó $u = v$.

$$x^2 = 5u + 4 \geq 0 \Rightarrow u \geq -\frac{4}{5}$$

$$y^2 = 10 - 6v \Rightarrow v \leq \frac{5}{3}.$$

Suy ra: $u = v = 0$ hoặc $u = v = 1$.

$u = v = 0 \Rightarrow y^2 = 10$, không có y nguyên nào.

$u = v = 1 \Rightarrow x^2 = 9$

$y^2 = 4$

Phương trình có bốn nghiệm: $(x = \pm 3; y = \pm 2)$ □

Thí dụ 3: Giải phương trình

$$x^2 + y^2 = 3z^2.$$

∇ Ta thấy ngay rằng phương trình có nghiệm là (0; 0; 0).

Giả sử phương trình có nghiệm $(x; y; z)$ khác (0; 0; 0).

Nếu x, y, z có ước chung lớn nhất là $d \neq 1$, tức $x = dx'$, $y = dy'$, $z = dz'$, với $(x', y', z') = 1$, thì:

$$(dx')^2 + (dy')^2 = 3(dz')^2 \Leftrightarrow x'^2 + y'^2 = 3z'^2.$$

Vì vậy có thể giả thiết x, y, z *nguyên tố cùng nhau.*

Từ $\quad x^2 + y^2 = 3z^2,$

ta có: $\quad x^2 + y^2 \vdots 3$

suy ra: $\quad x^2 \vdots 3$ và $y^2 \vdots 3$, tức $x = 3u$, $y = 3v$ và có:

$$(3u)^2 + (3v)^2 = 3z^2$$

$$3(u^2 + v^2) = z^2$$

Đẳng thức này chứng tỏ $z^2 \vdots 3$, tức $z \vdots 3$. Cả ba số x, y, z đều chia hết cho 3, trái với giả thuyết vừa nêu.

Vậy phương trình không thể có nghiệm nào khác (0; 0; 0) □

Thí dụ 4- Tìm nghiệm nguyên dương của phương trình

$$x + y + z = xyz$$

∇ Giả sử $0 < x \leq y \leq z$

Thế thì $x + y + z \leq 3z$.

Mà $x + y + z = xyz$

do đó $xyz \leq 3z$, *tức* $xy \leq 3$.

Nếu $x = y = z$ thì $z^3 = 3z$, $z^2 = 3$, là điều không thể có với z nguyên. Vậy phải có ít nhất hai trong ba số x, y, z không bằng nhau, do đó $xy < 3$, tức $xy = 2$ hoặc $xy = 1$.

$$xy = 2 \Rightarrow x = 1, y = 2 \Rightarrow z = 3$$

$$xy = 1 \Rightarrow x = y = 1 \Rightarrow 2 + z = z \text{ (vô nghiệm).}$$

Vậy phương trình đã cho có nghiệm là $(x = 1; y = 2; z = 3)$.

Vì vai trò của x, y, z là như nhau, nên ta có sáu nghiệm:

(1; 2; 3), (1; 3; 2), (2; 1; 3), (2; 3; 1), (3; 1; 2), (3; 2; 1). □

Chú ý- Mỗi phương trình Diophante tương đương với một hệ phương trình đồng dư.

Thí dụ- Phương trình

$$x^3 + 5y + 1 = 0$$

tương đương với hệ phương trình đồng dư:

$$x^3 + 1 \equiv 0 \pmod 5$$

$$y = \frac{x^3 + 1}{-5}$$

∇ Thực vậy, phương trình $x^3 + 1 \equiv 0 \pmod 5$

có nghiệm duy nhất là: $x \equiv -1 \pmod 5$

tức là $x = -1 + 5t$, $t \in \mathbb{Z}$

Do đó hệ phương trình trên có nghiệm là:

$$x = -1 + 5t$$

$$y = \frac{(-1+5t)^3+1}{-5} = -3t + 15t^2 - 25t^3$$

với $t \in \mathbf{Z}$. Đây cũng chính là công thức tổng quát cho nghiệm của phương trình Diophante đã cho. □

3.2 - Nói chung, giải *phương trình Diophante bậc cao* là một bài toán rất khó. Chú ý rằng nhiều khi ta gặp hai phương trình tương tự, chỉ khác nhau về hệ số, mà phương trình này có vô số nghiệm, phương trình kia lại vô nghiệm; phương trình này rất dễ giải, trong khi phương trình kia lại rất khó giải, thậm chí chưa ai giải được. Nhiều phương trình mang tên người đã giải được nó. Rất nhiều phương trình Diophante phải giải bằng các phương pháp của toán học cao cấp; việc nghiên cứu về phương trình Diophante đã trở thàng một ngành riêng được gọi là *giải tích Diophante.*

Sau đây là một vài thí dụ:

Có thể chứng minh dễ dàng rằng các phương trình:

$$2x^2 + y^2 = z^2$$

$$x^2 + y^2 = 2z^2$$

có thể đưa về phương trình $x^2 + y^2 = z^2$ và do đó có vô số nghiệm nguyên, nhưng phương trình

$$x^2 + y^2 = 3z^2$$

lại không có nghiệm nguyên nào (khác 0).

Có thể dễ dàng tìm điều kiện (cần và đủ) cho số tự nhiên k để phương trình:

$$x^2 - y^2 = k$$

không có nghiệm nguyên ($k \neq 4t + 2$), nhưng bài toán tương tự với phương trình

$$x^2 + y^2 = k$$

lại là bài toán rất khó !

Phương trình

$$x^2 + x - y^2 = 0$$

không có nghiệm nguyên; điều đó có thể chứng minh không khó; nhưng việc chứng minh rằng phương trình

$$x^2 + x - 2y^2 = 0$$

có vô số nghiệm nguyên: (8; 6), (49; 35),...lại là một bài toán rất khó !

Dễ thấy rằng phương trình

$$x^3 + y^3 + z^3 = 1$$

có vô số nghiệm nguyên ($x = 9n^4$; $y = 1 - 9n^3$; $z = 3n - 9n^4$), và phương trình

$$x^3 + y^3 + z^3 = 2$$

cũng có vô số nghiệm nguyên ($x = 1 + 6n^3$; $y = 1 - 6n^3$; $z = -6n^3$). Nhưng rất khó chứng minh rằng phương trình

$$x^3 + y^3 + z^3 = 3$$

có hay không có nghiệm nguyên nào khác ngoài bốn nghiệm là (1; 1; 1), (4; 4; -5), (4; -5; 4), và (-5; 4; 4).

Còn phương trình

$$x^3 + y^3 + z^3 = 30$$

có nghiệm nguyên hay không, đó là một bài toán rất khó.

Đối với hai phương trình khá đơn giản:

$$x^2 - y^3 = 1$$

$$x^2 - y^3 = -2$$

mà ta có thể thấy ngay được một nghiệm là (3; 2) đối với phương trình thứ nhất và (5; 3) đối với phương trình thứ hai, việc chứng minh rằng các phương trình đó không có nghiệm nào khác là điều không đơn giản chút nào !

Một dạng phương trình Diophante bậc hai nổi tiếng là phương trình

$$x^2 - Dy^2 = 1$$

trong đó D là số tự nhiên không chính phương (nếu D là số chính phương thì rất đơn giản), được gọi là *phương trình Pell.*

Thí dụ: $x^2 - 2y^2 = 1$

$x^2 - 29y^2 = 1.$

Phương trình Pell xuất phát từ một bài toán do Archimède (Ac-si-met, nhà bác học vĩ đại cổ Hy Lạp, sống ở thế kỉ thứ 3 trước Công nguyên) đặt ra, bài toán chứa 8 ẩn số thỏa mãn 7 phương trình, đưa đến việc tìm nghiệm nguyên của phương trình

$$x^2 - 4729494y^2 = 1 \quad (1)$$

Đương nhiên các nhà toán học cổ Hy Lạp không thể giải được phương trình này. Nhiều nhà toán học sau đó đã đi tìm lời giải. Có lẽ Fermat là người đầu tiên nói rõ là phương trình có vô số nghiệm. Nhà toán học Pháp Lagrange (La-gơ-răng) là người đầu tiên công bố lời giải đầy đủ của phương trình $x^2 - Dy^2 = 1$ năm 1766. Nhưng do một nhầm lẫn của Euler mà phương trình mang tên Pell, một nhà toán học Anh cùng thời. Phép giải phương trình Pell dựa vào lí thuyết về liên phân số.

Chú ý rằng năm 1880, người ta đã tìm ra nghiệm nguyên dương nhỏ nhất của phương trình (1), với x là một số gồm 45 chữ số và y là một số gồm 38 chữ số! Ngày nay, nếu không biết gì về phương pháp giải phương trình Pell, ta vẫn có thể nhờ máy tính điện tử để tìm nghiệm của (1):

$$x^2 = 4729494y^2 + 1$$

bằng cách cho y các giá trị tự nhiên liên tiếp: 1, 2, 3,...mỗi lần ta tính $4729494y^2 + 1$, rồi lấy căn bậc hai của số có được, cho đến bao giờ được căn đó là một số tự nhiên thì dừng lại; và

ta có nghiệm tự nhiên nhỏ nhất cần tìm. Máy tính điện tử có thể thực hiện hàng triệu phép tính trong một giây, nên sẽ tìm được nghiệm trong một thời gian rất ngắn.

Các bạn đừng nghĩ rằng việc giải phương trình Diophante chỉ là một trò tiêu khiển (dù rất đau đầu!) với các con số.

Các phương trình Diophante, ngoài những liên hệ về lí thuyết với những vấn đề khác, còn có những ứng dụng trong kĩ thuật; riêng phương trình Pell đã được gặp trong thiên văn học.

Bài tập

Giải các phương trình sau đây:

3.21 - $x^2 + y^2 = 2z^2$

3.22 - $x^2 + 2y^2 = z^2$

3.23 - $x^2 + y^2 = z^2 + 1$

3.24 - $x^2 - 4y^2 = 1$

3.25 - $x^2 - y^2 = 91$

3.26 - $2x^2 + 3y^2 = z^2$

3.27 - $x^2 + x - y^2 = 0$

3.28 - $x^3 + 7y = y^3 + 7x$

3.29 - $3x^2 + 10xy + 8y^2 = 96$

3.30 - $19x^2 + 28y^2 = 729$

3.31 - $xy + 3x - 5y = -3$

3.32 - $x + y = xy$

3.33 - $x + y + 1 = xyz$ (nghiệm nguyên dương)

3.34 - $x^3 - 2y^3 - 4z^3 = 0$

3.35 - $y^2 = x^3 + 7$

3.36 - $x^2 + y^2 + z^2 = x^2 y^2$

3.37 - $x^2 + y^2 + z^2 = 2xyz$

3.38 - $x^2 + y^2 + z^2 + u^2 = 2xyzu$

3.39 - $x^2 + y^2 + z^2 = u^2$ (nghiệm nguyên dương)

3.40 - $x^2 + y^2 + z^2 + u^2 = t^2$ (nghiệm nguyên dương)

3.41 - $8x^4 + 4y^4 + 2z^4 = t^4$

3.42 - $x(x + 1)(x + 7)(x + 8) = y^2$

3.43 - $x^2 + 5 = y^3$

3.44 - $x^6 + 3x^3 + 1 = y^4$

3.45 - $(x + 2)^4 - x^4 = y^3$

3.46 - $x_1^4 + x_2^4 + \ldots + x_{14}^4 = 1599$

3.47 - Tìm điều kiện (cần và đủ) cho số k để phương trình

$$x^2 - y^2 = k$$

có (ít nhất một) nghiệm nguyên.

3.48 - Tìm điều kiện (cần và đủ) cho số k để phương trình

$$x^3 + y^3 - z^3 = k$$

có nghiệm nguyên.

3.49 - Chứng minh rằng phương trình

$$x^2 - Dy^2 = 1$$

có vô số nghiệm nếu $D = m^2 + 1$ (m nguyên dương).

3.50 - Cho phương trình

$$x^2 + (x + 1)^2 = y^2.$$

Chứng minh rằng nếu $(x_0; y_0)$ là một nghiệm nguyên dương của phương trình thì

$$(3x_0 + 2y_0 + 1; 4x_0 + 3y_0 + 2)$$

cũng là một nghiệm của phương trình. Từ đó, hãy tìm ba nghiệm khác nhau của phương trình.

3.51 - Cho phương trình

$$x^2 + x - 2y^2 = 0$$

Chứng minh rằng nếu $(x_0; y_0)$ là một nghiệm nguyên dương của phương trình thì

$$(3x_0 + 4y_0 + 1; 2x_0 + 3y_0 + 1)$$

cũng là một nghiệm. Hãy tìm ba nghiệm nguyên dương khác nhau của phương trình.

3.52 - Tương tự bài 3.51, nếu cho phương trình

$$x^2 + x + 1 = 3y^2$$

và ta có nghiệm ($7x_0 + 12y_0 + 3;\ 4x_0 + 7y_0 + 2$) từ nghiệm nguyên dương $(x_0; y_0)$.

3.53 - Tương tự bài 3.51, nếu cho phương trình

$$x^2 - 2y^2 = 1$$

và ta có nghiệm $(3x_0 + 4y_0;\ 2x_0 + 3y_0)$ từ nghiệm nguyên dương $(x_0; y_0)$.

3.54 - Tìm nghiệm nguyên dương của phương trình:

$$\frac{1}{x^2} + \frac{1}{y^2} + \frac{1}{z^2} + \frac{1}{u^2} = 1.$$

3.55 - Tìm nghiệm nguyên dương của phương trình:

a) $\frac{1}{x} + \frac{1}{y} + \frac{1}{z} = 2.$

b) $\frac{1}{x} + \frac{1}{y} + \frac{1}{z} + \frac{1}{t} = 1.$

3.56 - Chứng minh rằng phương trình

$$\frac{1}{x} + \frac{1}{y} + \frac{1}{z} = \frac{1}{1991}$$

chỉ có một số hữu hạn nghiệm nguyên dương.

3.57 - Tìm nghiệm nguyên của:

a) $\frac{1}{x} + \frac{1}{y} = \frac{1}{14}.$

b) $\frac{1}{x} + \frac{1}{y} = \frac{1}{z}.$

3.58 - Tìm nghiệm nguyên của phương trình

$$1! + 2! + ... + x! = y^2.$$

CHƯƠNG 4

HỆ GHI SỐ NHỊ PHÂN ĐẠI SỐ MỆNH ĐỀ VÀ MÁY TÍNH

Một trò chơi : "đoán số"

Tôi ghi một số từ 1 đến 15, bạn không biết là số nào(tôi ghi vào mảnh giấy đây,gấp lại để trước mặt bạn).Bạn thử hỏi tôi để biết được số đó là số nào.Xin lưu ý rằng tôi sẵn sàng trả lời mọi câu hỏi của bạn,nhưng chỉ bằng một tiếng:"đúng" hoặc "sai" mà thôi.

Đương nhiên có thể đặt câu hỏi:

-Đó là số 0 ?

-Đó là số 1 ?

-Đó là số 2 ?

v.v...

Rõ ràng đặt câu hỏi như vậy,bạn chỉ " cầu may" thôi.May mắn lạ kì thì bạn hỏi mới có một câu đã biết ngay được số tôi đã ghi,nhưng không may thì bạn phải hỏi đến 16 câu.

Có một cách đặt câu hỏi hợp lí,"tiết kiệm" nhất,bảo đảm hỏi 4 câu thì rõ được số chưa biết.

V Bạn phải xác định một số trong 16 số,ta gọi "miền chưa biết" gồm 16 số.Bạn phải hỏi một câu sao cho sau khi tôi

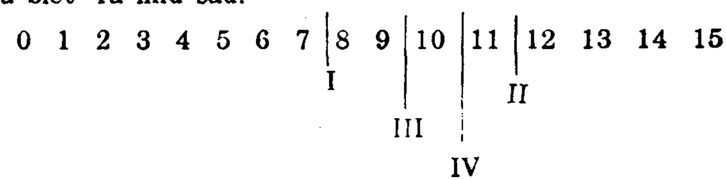
trả lời "đúng" hay "sai","miền chưa biết" sẽ thu hẹp còn một nửa,tức là chỉ còn 8 số.Muốn vậy,bạn có thể hỏi:

Câu hỏi I:Đó là số ≥ 8 ?

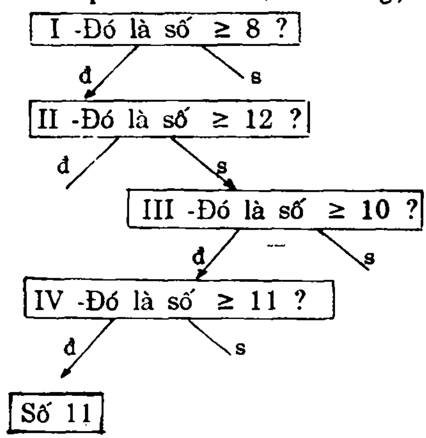
Nếu" đúng" thì "miền chưa biết" chỉ còn 8 số,từ 8 đến 15.Nếu"sai" thì "miền chưa biết" cũng chỉ là 8 số,từ 0 đến 7.

Tiếp theo,bạn chia "miền chưa biết" mới thành hai nửa,mỗi nửa gồm 4 số,để đặt câu hỏi II,sau câu hỏi II"miền chưa biết" chỉ còn 4 số;tiếp tục như vậy sau câu hỏi III thì "miền chưa biết" chỉ còn 2 số,và sau câu hỏi IV,miền chưa biết chỉ là một số. ❐

Nếu tôi ghi số 11 thì các câu hỏi của bạn đã chia" miền chưa biết" ra như sau:



Có thể thấy rõ hơn qua sơ đồ sau(đ là *đúng*,s là *sai):*



Việc đặt câu hỏi như vậy trong trò chơi trên đây dựa vào hệ ghi số nhị phân (cơ số 2),một hệ ghi số có ý nghĩa rất quan trọng trong lí thuyết và trong thực tế,với việc ra đời và phát triển của máy tính điện tử.

■ 1- Hệ ghi cơ số mười (thập phân)

1.1 -Chúng ta đã quá quen thuộc với cách ghi số và đọc các số đó.Thí dụ: số 2636

được đọc là *hai nghìn sáu trăm ba mươi sáu*,có nghĩa là

2	6	3	6
2.10^3	6.10^2	3.10	6

$$2636 = 2.10^3 + 6.10^2 + 3.10 + 6$$

Như vậy,trong cách ghi một số có nhiều chữ số thì kể từ phải sang trái:

- *chữ số đầu tiên* (hàng thứ 1) có giá trị bằng *chính nó,*
- *chữ số thứ hai* (hàng thứ hai) có giá trị bằng nó *nhân với 10,*
- *chữ số thứ ba* (hàng thứ ba) có giá trị bằng nó *nhân với* $100=10^2$,

....

- *chữ số thứ k* (hàng thứ *k*) có giá trị bằng chính nó *nhân với* 10^{k-1}.

Mỗi chữ số *vừa có giá trị riêng của nó,vừa có giá trị theo vị trí của nó trong biểu diễn số*.Cách biểu diễn số như vậy là cách biểu diễn theo *nguyên tắc vị trí.*

Ta so sánh với cách biểu diễn số la mã,trong đó mỗi chữ số đứng ở đâu cũng luôn có giá trị bằng chính nó. Thí dụ:

I = 1

III = 1 + 1 + 1 = 3

Trong khi đó: $111 = 1.10^2 + 1.10 + 1$

(chữ số 1 ở hàng thứ nhất từ phải sang trái bằng chính nó,nhưng chữ số 1 ở hàng thứ hai lại bằng nó nhân với 10,...)

Một cách tổng quát,có thể chứng minh được rằng:

Mọi số N $\neq 0$ đều có thể viết một cách duy nhất dưới dạng tổng các luỹ thừa của 10,mỗi luỹ thừa có hệ số là số tự nhiên nhỏ hơn 10 (riêng $a_n \neq 0$).

$$N = a_n . 10^n + a_{n-1} . 10^{n-1} + ... + a_2 . 10^2 + a_1 . 10 + a_0$$

và được kí hiệu là:

$$N = \overline{a_n a_{n-1} \ldots a_2 a_1 a_0}$$

(gạch ngang trên đầu để phân biệt với tích của các số $a_n, a_{n-1}, ..., a_2, a_1, a_0$).

Ta dùng mười chữ số :0, 1, 2, ...,8,9 để biểu diễn mọi số,lấy các *luỹ thừa của 10* để xác định giá trị của chữ số theo vị trí của nó trong biểu diễn số. Đây là *hệ ghi số theo cơ số 10*, cũng thường gọi là *hệ ghi số thập phân.*

Trong trường hợp N có ít chữ số,ta thường kí hiệu các chữ số của nó là *a, b, c, d* hoặc *x, y, z*...

Thí dụ: Tìm số có ba chữ số, biết rằng khi viết thêm 1 vào bên phải số đó thì được một số gấp ba lần số có được bằng cách viết thêm 2 vào bên trái của số đó.

∇ Số phải tìm có dạng $\overline{abc}$

Thêm 1 vào bên phải của *x*, có số $\overline{abc1}$

Thêm 2 vào bên trái của *x*, có số $\overline{2abc}$

Theo đề bài,ta có:

$$\overline{abc1} = 3 . \overline{2abc}$$

$a \cdot 10^3 + b \cdot 10^2 + c \cdot 10 + 1 = 3(2 \cdot 10^3 + a \cdot 10^2 + b \cdot 10 + c)$

Rút gọn,được:

$$700a + 70b + 7c = 5999$$

$$100a + 10b + c = 857$$

Mà $100a + 10b + c = \overline{abc}$

nên $x = \overline{abc} = 857$. □

Bài tập

4.1 -Cần bao nhiêu chữ số để đánh số trang của một cuốn sách dày 326 trang ?

4.2 -Để đánh số trang một cuốn sách,phải dùng tất cả 824 chữ số.Cuốn sách có bao nhiêu trang ?

4.3 -Tìm $N = \overline{xyzt}$,biết $N = \overline{xz} + 2\overline{yzt}$.

4.4 -Tìm giá trị lớn nhất của $\dfrac{\overline{xyz}}{x + y + z}$

4.5 -Cho biết

$M = \overline{7a_n \ldots a_0} = 5\overline{a_n \ldots a_0 7}$.

Tìm giá trị nhỏ nhất của M.

4.6 -Tìm $N = \overline{abcd}$, biết rằng a, $\overline{cd}$, $\overline{ad}$ và N đều là số chính phương.

4.7 -Tìm một số có hai chữ số biết rằng:

- tổng các chữ số của nó không nhỏ hơn 7,
- tổng các bình phương của các chữ số của nó không lớn hơn 30,
- hai lần số viết theo chiều ngược lại không lớn hơn số đã cho.

4.8 -Tìm các số có hai chữ số,biết rằng số đó là bội của tích hai chữ số của nó.

4.9 -Số P gồm có 6 chữ số.Chứng minh rằng P chia hết cho 7 khi và chỉ khi hiệu giữa số tạo bởi ba chữ số đầu và số tạo bởi ba chữ số cuối của P chia hết cho 7.

4.10 -Tổng các chữ số của một số có ba chữ số chia hết cho 7.Chứng minh rằng số ấy chia hết cho 7 khi và chỉ khi chữ số hàng đơn vị và chữ số hàng chục bằng nhau.

4.11 -Chứng minh rằng $M = \overline{a_n \ldots a_1 a_0}$ chia hết cho 13 khi và chỉ khi $4a_0 + \overline{a_n \ldots a_1}$ chia hết cho 13.

4.12 -Chứng minh rằng điều kiện cần và đủ để số $M = \overline{a_n \ldots a_1 a_0}$ chia hết cho 17 là $3\overline{a_n \ldots a_1} + 2a_0$ chia hết cho 17.

4.13 -a)Tìm các chữ số *x*,*y* để cho số $\overline{1234xy}$ chia hết cho 8 và cho 9.

b) Tìm chữ số *x* để số $\overline{2x78}$ chia hết cho 17.

4.14 -Lấy một số có ba chữ số trừ đi tổng các chữ số của nó, rồi tiếp tục làm như vậy đối với số mới.

Chứng minh rằng kết quả cuối cùng bằng 0.

■ 2 - Hệ ghi cơ số g bất kì

2.1 -Trong hệ ghi số quen thuộc (thập phân),ta dùng *mười chữ số* và lấy các *luỹ thừa của mười* để xác định giá trị theo vị trí của chữ số trong biểu diễn số.

Bây giờ,nếu ta dùng không phải mười chữ số mà chỉ *bảy chữ số*

$$0,\ 1,\ 2,\ 3,\ 4,\ 5,\ 6$$

và lấy các *luỹ thừa của bảy* để xác định giá trị theo vị trí của chữ số trong biểu diễn số,thì ta có *hệ ghi theo cơ số bảy.*

Thí dụ, nếu biểu thức

$$2.10^2 + 3.10 + 6$$

được ghi là 236 (*cơ số mười*) hay chỉ đơn giản là 236,

thì biểu thức

$$2.7^2 + 3.7 + 6$$

sẽ được ghi là

$$236\ (\textit{cơ số bảy})\ \text{hay là}\ 236_7$$

(số 7 viết nhỏ ở dưới là số trong hệ thập phân, chứ trong hệ cơ số bảy không có chữ số 7).

Ta có:

$$2.7^2 + 3.7 + 6 = 98 + 21 + 6 = 125$$

Vì vậy 236_7 và 125 là hai cách biểu diễn khác nhau của cùng một số trong hai hệ ghi theo cơ số khác nhau.

Tương tự, nếu ta chỉ dùng bốn chữ số

$$0,\ 1,\ 2,\ 3$$

và lấy các luỹ thừa của 4 để xác định giá trị theo vị trí của chữ số trong biểu diễn số ,thì ta có hệ ghi cơ số 4.

Thí dụ , biểu thức:

$$3.4^2 + 1.4 + 2\ (= 48 + 4 + 2 = 54)$$

được kí hiệu là 312_4.

54 và 312_4 biểu diễn cùng một số,trong hai hệ ghi cơ số khác nhau:

trong hệ thập phân, đó là 54 (đọc: năm *mươi* bốn);

trong hệ ghi cơ số bốn, đó là 312 (đọc: *ba một hai,cơ số bốn).*

Số 10231_4 có giá trị như sau:

$$\begin{array}{ccccc} 1 & 0 & 2 & 3 & 1 \\ 1.4^4 & 0.4^3 & 2.4^2 & 3.4 & 1 \end{array}$$

$$\begin{aligned} 10231_4 &= 1.4^4 + 0.4^3 + 2.4^2 + 3.4 + 1 \\ &= 256 + 0 + 32 + 12 + 1 = 301. \end{aligned}$$

Như vậy, 10231_4 và 301 biểu diễn cùng một số trong hai hệ ghi theo cơ số khác nhau:

trong hệ cơ số 4,đó là 10231_4 (đọc:một không hai ba một,cơ số bốn)

trong hệ thập phân, đó là 301 (ba trăm lẻ một).

2.2 -Một cách tổng quát,ta có:

Định lí *Với số tự nhiên g > 1 tuỳ ý cho trước thì mỗi số tự nhiên N ≠ 0 đều biểu diễn được một cách duy nhất thành một tổng của những luỹ thừa của g,với các hệ số là số tự nhiên nhỏ hơn g.*

$$N = a_n g^n + a_{n-1} g^{n-1} + \dots + a_2 g^2 + a_1 g + a_0$$

trong đó $0 \le a_{n-1}; \dots a_2; a_1, a_0 < g$,

riêng $0 < a_n < g$.

∇ Chia N cho g,theo định lí về *phép chia có dư*, ta có cặp số duy nhất $(M_1; a_0)$ sao cho:

$$(1)\ N = M_1 . g + a_0\ (0 \le a_0 < g$$

Chia M_1 cho g,có *cặp số duy nhất* $(M_2; a_1)$:

$$M_1 = M_2 . g + a_1\ (0 \le a_1 < g)$$

Thay vào (1),được:

$$N = (M_2 g + a_1) g + a_0$$

$$= M_2 g^2 + a_1 g + a_0$$

Lại chia M_2 cho g,có *cặp số duy nhất* $(M_3;a_2)$:

$$M_2 = M_3 . g + a_2\ (0 \le a_2 < g)$$

Thay vào (2),được:

$$N = (M_3 g + a_2) g^2 + a_1 g + a_0$$

$$= M_3 g^3 + a_2 g^2 + a_1 g + a_0.$$

Tiếp tục như vậy,ta có:

$$M > M_1 > M_2 > M_{3...}>...$$

và phải đến lúc có $0 < M_n < g$. Lấy $M_n = a_n$, ta được đẳng thức phải chứng minh:

$$N = a_n g^n + a_{n-1} g^{n-1} + \ldots + a_2 g^2 + a_1 g + a_0.$$

Người ta biểu diễn số N dưới dạng:

$$N = (a_n a_{n-1} \ldots a_2 a_1 a_0)_g.$$

(có thể bỏ dấu ngoặc ở hai đầu).Đây là kí hiệu của số N trong hệ ghi cơ số g.

$a_n, a_{n-1}, \ldots, a_2, a_1, a_0$ là các chữ số, mỗi chữ số là một số tự nhiên < g, riêng $0 < a_n < g$.

Riêng với g = 10, số N được kí hiệu là:

$$N = \overline{a_n a_{n-1} \ldots a_2 a_1 a_0}.$$

Cần ghi nhớ:

Trong hệ cơ số g ,để biểu diễn một số N bất kì :

- ta dùng g chữ số:

0, 1, 2, ... , g-1

- ta lấy các luỹ thừa của g để xác định giá trị của mỗi chữ số theo vị trí của nó trong N; kể từ phải sang trái:

chữ số đầu tiên (hàng thứ nhất) có giá trị bằng chính nó,

chữ số thứ hai (hàng thứ hai) có giá trị bằng nó nhân với g ,

chữ số thứ ba (hàng thứ ba) có giá trị bằng nó nhân với g^2,

chữ số thứ k (hàng thứ k) có giá trị

bằng nó nhân với g^{k-1}

Thí dụ:

$$N = (uvxyz)_g$$

Hàng thứ 5	Hàng thứ 4	Hàng thứ 3	Hàng thứ 2	Hàng thứ 1
u	v	x	y	z
$u.g^4$	$v.g^3$	$x.g^2$	$y.g$	z

$$N = u.g^4 + v.g^3 + x.g^2 + y.g + z.$$

Trường hợp $g = 2$ *(hệ cơ số 2 hay nhị phân)*

Ta chỉ dùng chữ số 0 và 1 để biểu diễn mọi số.

$$N = 1.2^3 + 0.2^2 + 1.2 + 1$$

$$= 8 + 0 + 2 + 1 = 11$$

được kí hiệu là 1011_2 (đọc: *một không một một,cơ số hai)*

Ta có $1011_2 = 11$.

Trường hợp $g = 3$ *(hệ cơ số 3 hay tam phân)*

Ta chỉ dùng ba chữ số là 0, 1, 2 để biểu diễn mọi số.

Số 11 (hệ thập phân) có thể biểu diễn dưới dạng tổng các luỹ thừa của 3 như sau:

$$11 = 1.3^2 + 0.3 + 2$$

và được kí hiệu là 102_3 (đọc: *một không hai,cơ số ba)*

Như vậy,ta có

$$11 = 1011_2 = 102_3$$

nghĩa là cùng một số, được biểu diễn

trong hệ thập phân là 11

trong hệ nhị phân là 1011_2

trong hệ tam phân là 102_3.

Trường hợp *g = 12 (hệ cơ số 12)*

Để biểu diễn mọi số,ta dùng 12 chữ số. Ngoài 10 chữ số là 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, ta phải chọn thêm hai kí hiệu nữa riêng cho 10 và 11.Người ta thường lấy:

A để ghi số 10

B để ghi số 11.

Như vậy, biểu thức

$$10.12^2 + 11.12 + 7$$

A B 7

được kí hiệu là: $AB7_{12}$ (đọc: *A B bảy,cơ số mười hai)*

Vì $10.12^2 + 11.12 + 7 = 1440 + 132 + 7 = 1579$,

nên ta có

$$AB7_{12} = 1579$$

Với số $2B0A_{12}$, ta có:

2	B	0	A
2.12^3	$B.12^2$	0.12	A

$$2B0A_{12} = 2.12^3 + 11.12^2 + 0.12 + 10$$
$$= 2.1728 + 11.144 + 0 + 10 = 5050$$

Hệ cơ số 12 hiện còn sử dụng ở một số nơi. Bạn ra chợ, thỉnh thoảng nghe những người mua bán trái cây, bắp, trứng,... hỏi nhau;"Chục mười hay chục mười hai?".Chục mười hai là một tá, mỗi tá gồm 12 đơn vị.

Chú ý rằng trong hệ cơ số g,

số g được biểu diễn bởi 10_g

số g^2 được biểu diễn bởi 100_g

Tổng quát: số g^k được biểu diễn bởi $10...0_g$ (k chữ số 0)

Trong hệ cơ số 2 (nhị phân):

$2 = 1.2 + 0 = 10_2$

$4 = 2^2 = 1.2^2 + 0.2 + 0 = 100_2$

$8 = 2^3 = 1.2^3 + 0.2^2 + 0.2 + 0 = 1000_2$

$16 = 2^4 = 1.2^4 + 0.2^3 + 0.2^2 + 0.2 + 0 = 10000_2$

Trong hệ cơ số 3:

$10_3 = 3$

$100_3 = 3^2 = 9$

$10000_3 = 3^4 = 81$

Trong hệ cơ số 12:

$10_{12} = 12$

$100_{12} = 12^2 = 144$

2.3- Đổi một số được viết trong hệ cơ số này sang hệ cơ số khác

a) Đổi một số trong hệ cơ số g tuỳ ý sang hệ thập phân

Trên đây,chúng ta đã nhiều lần thực hiện việc chuyển đổi này bằng cách viết số đã cho dưới dạng một tổng các luỹ thừa của cơ số g (viết trong hệ thập phân).Thí dụ:

$3214_5 = 3.5^3 + 2.5^2 + 1.5 + 4 = 375 + 50 + 5 + 4 = 434$

Ta có thể đổi theo cách khác, trong nhiều trường hợp là tiện lợi hơn, theo sơ đồ sau đây (áp dụng cho số 3214_5):

$$
\begin{array}{l}
3 \\
\times\ 5 \\
\hline
15 + 2 = 17 \\
\qquad\quad \times\ 5 \\
\qquad\quad \overline{85 + 1 = 86} \\
\qquad\qquad\qquad \times\ 5 \\
\qquad\qquad\qquad \overline{430 + 4 = 434}
\end{array}
$$

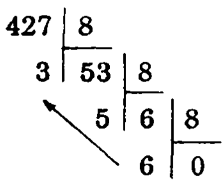
Có thể giải thích dễ dàng quy tắc sau đây :

Quy tắc- *Muốn đổi một số từ hệ cơ số g tuỳ ý sang hệ thập phân, ta lấy chữ số đầu tiên (từ trái sang phải) nhân với g, rồi cộng kết quả với chữ số thứ hai(từ trái sang phải), lấy tổng này nhân với g, rồi cộng kết quả với chữ số thứ ba,...tiếp tục như thế cho đến phép cộng với chữ số cuối cùng(từ trái sang phải) cho ta kết quả cần tìm.*

b) Đổi một số từ hệ thập phân sang hệ cơ số g khác

Thí dụ 1- Viết số 427 trong hệ cơ số 8.

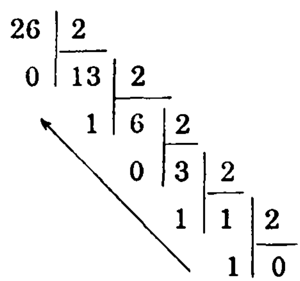
Ta chia 427 cho 8 (dư 3), rồi chia thương tìm được cho 8 (dư 5),...như sau :



Số phải tìm là 653_8, nghĩa là $427 = 653_8$.

Quy tắc- *Muốn đổi một số N từ hệ thập phân sang hệ cơ số g (khác 10), ta chia số N cho g, rồi chia thương tìm được cho g,..., cho đến khi có thương bằng 0. Các số dư có được, kể từ số dư cuối cùng trở lên số dư đầu tiên, là các chữ số từ trái sang phải của số phải tìm.*

Thí dụ 2- Viết số 26 trong hệ nhị phân.



Vậy $26 = 11010_2$.

Quy tắc đổi trên đây dựa vào *định lí :*

Mọi số N đều có thể viết dưới dạng

$$N = a_n g^n \ldots + a_2 g^2 + a_1 g + a_0$$

trong đó $0 \le a_{n-1}, \ldots, a_2, a_1, a_0 < g$ *và* $0 < a_n < g$.

Do đó,khi chia N cho g, ta được số dư là a_0 (đây là chữ số đầu tiên từ phải sang trái trong biểu diễn của N theo cơ số g), và thương là:

$$N_1 = a_n g^{n-1} + \ldots + a_2 g + a_1$$

Chia N_1 cho g, được số dư là a_1 (chữ số thứ hai trong biểu diễn của N theo cơ số g), v.v...

c) Đổi một số viết trong hệ cơ số a sang hệ sơ số b (a, b đều ≠ 10)

Ta đổi số đã cho từ hệ cơ số a sang hệ thập phân, sau đó đổi số từ hệ thập phân sang hệ cơ số b.

Thí dụ: viết số 3214_5 trong hệ cơ số 9.

Thực hiện theo các quy tắc biến đổi ở trên,ta được:

$3214_5 = 434$

$434 = 532_9$

Vậy $3214_5 = 532_9$

Bài tập

4.15 -Viết các số sau đây dưới dạng tổng các luỹ thừa của cơ số:

a) 6015_7 b) 312_4 c) 43012_5

d) 8765_9 e) $3A05_{11}$ g) $ABA1_{12}$

4.16 -Viết các số (theo cơ số g tương ứng) biểu diễn các tổng sau đây:

a) $2.3^3 + 3^2 + 3 + 1$ (g = 3)

b) $2^4 + 2^3 + 2 + 1$ (g = 2)

c) $7.9^5 + 3.9 + 4$ (g = 9)

d) $11.13^3 + 10.13 + 10$ (g = 13)

4.17 a) Trong hệ cơ số nào, ta có:

$2 + 4 = 10$; $2 + 5 = 10$

$12 + 13 = 30$; $2 + 5 = 7$?

b) Tìm số lớn nhất:

- có một chữ số trong hệ cơ số 8
- có hai chữ số trong hệ cơ số 3
- có ba chữ số trong hệ cơ số 2
- có bốn chữ số trong hệ cơ số 5.

Viết các số tìm được trong hệ thập phân.

4.18 -Tìm các cơ số x, y biết rằng x, y ≤ 10 *và*:

a) $23_x = 32_y$ b) $51_x = 15_y$

4.19 -a) Tính các tổng sau đây (viết kết quả theo cơ số tương ứng và theo cơ số mười):

$2_3 + 1_3$; $2_3 + 2_3$; $3_4 + 2_4$; $45_6 + 51_6$

b) Tìm các chữ số thiếu ở chỗ các dấu chấm trong phép cộng sau:

$$\begin{array}{r} 2\,3\,.\,5\,. \\ 1\,.\,6\,4\,2 \\ \hline 4\,2\,4\,2\,3 \end{array}$$

4.20- Một thầy giáo nói :"Lớp tôi có 100 học sinh, trong đó có 24 nam và 32 nữ ".Thầy cộng không nhầm.Thế là thế nào ?

4.21- Chứng minh rằng:

a) 121 là số chính phương trong mọi hệ cơ số $g > 2$;

b) 144 là số chính phương trong mọi hệ cơ số $g > 4$;

c) 1311 là lập phương của một số tự nhiên trong mọi hệ cơ số $g > 3$.

4.22 -a) Tìm dấu hiệu chia hết cho 2, cho 3 trong hệ cơ số 6; dấu hiệu chia hết cho 2, cho 3, cho 4, cho 6 trong hệ cơ số 12. So sánh với các dấu hiệu chia hết cho 2, cho 5 trong hệ thập phân, có thể rút ra kết luận gì ?

b) Tìm dấu hiệu chia hết cho g – 1 va g + 1 trong hệ cơ số g.

4.23- a) Tìm cơ số của các hệ ghi số trong đó dấu hiệu chia hết của một số N cho số d là tổng các chữ số của N chia hết cho d.

b) Trong các hệ cơ số nào thì các dấu hiệu chia hết cho 3 và cho 9 giữ nguyên dấu hiệu như trong hệ thập phân quen thuộc ?

4.24- Chứng minh rằng trong bất kì hệ cơ số nào, các số 10101, 1010101 cũng là hợp số.

4.25- Tìm số có ba chữ số trong hệ thập phân, biết rằng số đó viết trong một hệ cơ số khác 10 thì bằng hai lần số đó viết trong hệ thập phân.

4.26- Viết các số sau đây sang số trong hệ thập phân:

1011011_2, 21012_3, 4517_8, 1328_9, AB_{12}

4.27 -Đổi các số sau đây sang số trong hệ cơ số 2, 3, 4, 5, 8:

25, 87, 195, 478.

4.28- Tìm x (số có nhiều chữ số), biết:

$101_2 = (x)_3$, $2101_3 = (x)_2$

$10110_2 = (x)_4$, $102432_5 = (x)_6$

4.29- Tìm g , biết:

a) $231 = 3213_g$; b) $2345_6 = 652_g$

■ 3 - Hệ nhị phân (cơ số 2)

3.1- Hệ nhị phân có rất nhiều ứng dụng, do chỉ dùng hai kí hiệu 0 và 1, và việc tính toán với các số trong hệ này rất đơn giản .

Trong hệ thập phân, để làm tính cộng và nhân, ta phải thuộc lòng nhiều bảng, nhất là các *bảng nhân* (nhân với 2,

nhân với 3,..., nhân với 9). Trong hệ nhị phân, chỉ cần có *một bảng cộng và một bảng nhân* vẻn vẹn mấy dòng như sau:

$0 + 0 = 0$	$0 \times 0 = 0$
$0 + 1 = 1$	$0 \times 1 = 0$
$1 + 0 = 1$	$1 \times 0 = 0$
$1 + 1 = 10$	$1 \times 1 = 1$
Bảng cộng	*Bảng nhân*

Các bảng này cũng thường được trình bày dưới dạng khác:

+	0	1
0	0	1
1	1	10

Bảng cộng

×	0	1
0	0	0
1	0	1

Bảng nhân

Như vậy, khi làm tính cộng và nhân, ta có thể thực hiện như trong hệ thập phân quen thuộc (nhưng đơn giản rất nhiều, vì luôn luôn chỉ có 0 và 1 !), chỉ lưu ý một điều duy nhất khi làm tính cộng:

Trong hệ thập phân (cơ số mười):

8 + 2 bằng mười, viết 0 nhớ 1

Trong hệ nhị phân (cơ số hai):

1 + 1 bằng hai, viết 0 nhớ 1.

(nhớ 1 sang chữ số hàng thứ hai bên trái).

Dễ dàng làm các phép tính cộng,trừ, nhân và chia các số trong hệ nhị phân, thí dụ:

$$\begin{array}{r} 10011 \\ +\ 11001 \\ \hline 101100 \end{array} \qquad \begin{array}{r} 101101 \\ -\ 10110 \\ \hline 10111 \end{array}$$

$$\begin{array}{r} 10101 \\ \times\ 1011 \\ \hline 10101 \\ 10101 \\ 101010 \\ \hline 11100111 \end{array} \qquad \begin{array}{r|l} 101101 & 11 \\ \cline{2-2} 101 & 1111 \\ 100 & \\ 11 & \\ 0 & \end{array}$$

Trong bài toán chia trên đây, ta có:

- chia 101 cho 11, được 1, dư 10: 101 = 11.1 + 10
- chia 100 cho 11, được 1, dư 1: 100 = 11.1 + 1.

3.2 - Trở lại "trò chơi đoán số" ở đầu chương này.

a) Giả sử ta quy ước: với các câu hỏi đã đặt ra ($x \geq 8$? $x \geq 12$? v.v..),

câu trả lời" đúng" được kí hiệu là 1

câu trả lời "sai" được kí hiệu là 0.

Thế thì sau khi hỏi 4 câu, ta được một dãy 4 chữ số 0 hay 1 biểu diễn số phải tìm trong hệ nhị phân. Thí dụ nếu tôi đã ghi số 11 thì các câu trả lời kế tiếp nhau phải là

	đúng	*sai*	*đúng*	*đúng*
tức là	1	0	1	1

Đây là kí hiệu của số 11 trong hệ nhị phân:

$$1011_2 = 1.2^3 + 1.2 + 1 = 11.$$

Có thể giải thích như sau:

Chú ý rằng $x < 16$ và:

$$8 = 2^3,\ 10 = 2^3 + 2,\ 12 = 2^3 + 2^2,$$

ta có:

1) Hỏi: "$x \geq 8$?".Trả lời: đúng

$\Rightarrow x \geq 2^3 \Rightarrow x = 1.2^3 + y \; (y < 2^3)$

2) Hỏi: "$x \geq 12$?".Trả lời: sai

$\Rightarrow x < 12 \Rightarrow x = 1.2^3 + 0.2^2 + z \; (z<2^2)$

3) Hỏi "$x \geq 10$?".Trả lời : đúng

$\Rightarrow x \geq 2^3 + 2 \Rightarrow x = 1.2^3 + 0.2^2 + 1.2 + t$

$(t < 2)$

4) Hỏi: "$x \geq 11$?". Trả lời: đúng

$\Rightarrow x = 11 \Rightarrow x = 1.2^3 + 0.2^2 + 1.2 + 1 = 1011_2.$

Tương tự như vậy với mọi x từ 0 đến 15.

b) Thay vì đặt câu hỏi $x \geq 8$?, $x \geq 12$?,v.v...,ta có thể đặt câu hỏi khác một chút, dựa vào qui tắc đổi một số từ hệ thập phân sang hệ nhị phân:

Câu hỏi 1: Bạn hãy chia x cho 2.
Số dư là 1, đúng không ? -Đúng: 1
-Sai: 0

Câu hỏi 2: Bạn hãy chia thương vừa tìm được cho 2.Số dư là 1, đúng không ? -Đúng: 1
-Sai: 0

Câu hỏi 3: Bạn hãy chia thương vừa tìm được (sau câu hỏi 2) cho 2.Số dư là 1, đúng không ? -Đúng: 1
-Sai: 0

Câu hỏi 4: Bạn hãy chia thương vừa tìm được (sau câu hỏi 3) cho 2.Số dư là 1, đúng không ? -Đúng: 1
-Sai: 0

Hỏi 4 câu thì dừng lại.Các kết quả (0 hay 1) từ câu hỏi 4 lên câu hỏi 1 là các chữ số liên tiếp (từ trái sang phải) của số x viết trong hệ nhị phân.Nếu kết quả các câu trả lời như sau:

câu hỏi 1 cho 1

câu hỏi 2 cho 1

câu hỏi 3 cho 0

câu hỏi 4 cho 1

thì số cần biết là

$$x = 1011_2 = 1.2^3 + 0.2^2 + 1.2 + 1 = 11.$$

3.3 - Do việc làm tính cộng và nhân các số trong hệ nhị phân rất đơn giản, ta có thể đổi một số từ hệ cơ số g bất kì sang hệ nhị phân bằng cách:

- Viết số đã cho dưới dạng lũy thừa của g (trong hệ thập phân);

- Đổi tất cả các hệ số và cơ số g sang hệ nhị phân (trừ các số mũ trong lũy thừa của g thì vẫn giữ trong hệ thập phân);

- Thực hiện (trong hệ nhị phân) các phép tính trong biểu thức có được; kết quả cuối cùng là kí hiệu cuả số đã cho trong hệ nhị phân.

Thí dụ 1. Viết số 221_3 trong hệ nhị phân.

Ta có: $221_3 = 2.3^2 + 2.3 + 1$

Mà $2 = 10_2$ và $3 = 11_2$

nên $221_3 = 10_2.{11_2}^2 + 10_2.11_2 + 1$

Ta tính được:

$${11_2}^2 = 11_2.11_2 = 1001_2$$

Vì vậy:

$$221_3 = 10_2.1001_2 + 10_2.11_2 + 1$$
$$= 10010_2 + 110_2 + 1 = 11001_2.$$

Thí dụ 2. Đổi số 541 ra số trong hệ nhị phân.

$$541 = 5.10^2 + 4.10 + 1.$$

Mà $5 = 101_2 \quad 4 = 100_2 \quad 10 = 1010_2$,

nên $541 = 101_2.1010_2{}^2 + 100_2.1010_2 + 1$

$$1010^2 = 1010 \,.\, 1010 = 1100100$$

Vậy $541 = 101_2.1100100_2 + 100_2.1010_2 + 1$

$$= 111110100_2 + 101000_2 + 1$$
$$= 1000011101_2.$$

3.4 - Hệ cơ số 8 và hệ cơ số 16 (hexa)

Hệ nhị phân có bất tiện là các số viết trong hệ này phải dùng quá nhiều chữ số và rất khó đọc. Vì vậy, trong ứng dụng thực tế, người ta hay dùng *hệ cơ số 8 và hệ cơ số 16.*

Việc đổi một số từ hệ cơ số 2 sang các hệ cơ số $4 = 2^2$, cơ số $8 = 2^3$, cơ số $16 = 2^4$ và ngược lại, là một vấn đề rất đơn giản.

Từ hệ cơ số 2 sang hệ cơ số 4

Thí dụ: đổi số 10110_2 thành số trong hệ cơ số 4. Ta tách 10110_2 thành từng nhóm gồm hai chữ số (kể từ phải sang trái, nhóm sau cùng có thể chỉ có một chữ số) rồi đổi như sau:

Số trong hệ cơ số 2:	1	01	10
Số trong hệ cơ số 4:	1	1	2

$$\text{Vậy } 10110_2 = 112_4$$

Ngược lại, đổi 2103_4 sang số trong hệ nhị phân:

Số trong hệ cơ số 4: 2 1 0 3

Số trong hệ cơ số 2: 10 01 00 11

Vậy $2103_4 = 10010011_2$

Chú ý rằng phải viết 1 = 01, 0 = 00 (gồm hai chữ số).

Ta có thể *chứng minh quy tắc chuyển đổi* trên đây như sau. Để đơn giản, ta lấy một số có 6 chữ số trong hệ nhị phân $(abcdeg)_2$:

$$(abcdeg)_2 = a.2^5 + b.2^4 + c.2^3 + d.2^2 + e.2 + g$$
$$= (2a + b).2^4 + (2c + d).2^2 + (2e + g)$$
$$= m.4^2 + n.4 + p$$

Các số m = 2a + b, n = 2c + d, p = 2e + g (đều < 4) chính là các số nhị phân gồm hai chữ số viết sang hệ cơ số 4, và đẳng thức trên đây cho ta

$$(abcdeg)_2 = (mnp)_4$$

Có thể mở rộng dễ dàng phép chứng minh trên đây cho số bất kì, và cho các quy tắc đổi một số từ hệ nhị phân sang hệ cơ số 8 và hệ cơ số 16 như dưới đây:

Từ hệ cơ số 2 sang hệ cơ số 8

Ta tách các chữ số của số viết trong hệ cơ số 2 thành *từng nhóm gồm 3 chữ số*, kể từ phải sang trái (nhóm sau cùng có thể không đủ 3 chữ số).

Số trong hệ cơ số 2: 10 011 001

Số trong hệ cơ số 8: 2 3 1

Vậy $10011001_2 = 231_8$

Số trong hệ cơ số 8: 1 7 3 2

Số trong hệ cơ số 2: 1 111 011 010

Vậy $1732_8 = 1111011010_2$

Chú ý: viết $2 = 010_2$, gồm *ba chữ số).*

Từ hệ cơ số 2 sang hệ cơ số 16

Đối với hệ cơ số 16, ta phải dùng 16 chữ số. Ngoài 10 chữ số từ 0 đến 9, người ta thường dùng A(10), B(11), C(12), D(13), E(14) và F(15). Thí dụ:

$$AD2_{16} = 10.16^2 + 13.16 + 2$$

Hệ cơ số 16 thường được gọi là *hệ hexa* và ghi chữ *h* ở cuối của số, thí dụ AD2*h*.

Việc đổi một số từ hệ cơ số 2 sang hệ hexa được thực hiện rất đơn giản như sau:

Số trong hệ cơ số 2:	101	0011	1011	
Số trong hệ hexa:	5	3	B	

Vậy $10100111011_2 = 53B_{16}$ (= 53Bh)

Số trong hệ hexa:	C	2	5	E
Số trong hệ cơ số 2:	1100	0010	0101	1110

Vậy C25Eh = 1100001001011110_2

Ngoài hệ cơ số 8 hay hệ hexa, người ta cũng dùng hệ thập phân với các chữ số được mã hóa nhị phân, có khi được gọi là *dạng nhị-thập phân* và kí hiệu là $(abcd)_{2\text{-}10}$.

Thí dụ:

Số trong hệ thập phân:	8	3	4
	1000	0011	0100

Số 834 được viết dưới dạng nhị-thập phân là

$$(1000\ 0011\ 0100)_{2\text{-}10}$$

(Chú ý rằng đây không phải là kí hiệu của số 834 trong hệ nhị phân)

Bài tập

4.30 - Đổi các số sau đây ra số trong hệ nhị phân:

17 76 463 1203 11355

4.31 - Đổi các số sau đây (trong hệ nhị phân) ra số trong hệ thập phân, hệ cơ số 4 và hệ cơ số 8:

10110 110101010 101011000110

4.32 - Đổi các số sau đây ra số trong hệ hexa:

a) 35 298 162065

b) cơ số 2: 10110 110101010 10101100011

4.33 - Đổi các số sau đây ra số trong hệ nhị phân và hệ thập phân:

D5h 9A2Bh

7BF52CEh 2A01BF59h

4.34 - Cho M = 1011 N = 11001

P = 100110 Q = 1000010011

Tính các biểu thức sau đây rồi kiểm tra lại kết quả trong hệ thập phân:

M + N, N - M + P, M.N, Q /M, Q - MN.

4.35 - Viết các số sau đây dưới dạng nhị-thập phân

47 506 2119

4.36 - a) Trong "trò chơi đoán số" (xem đầu chương), nếu ghi một số từ 0 đến 14 (một trong 15 số) thì có thể đặt câu hỏi như thế nào? Nếu đặt câu hỏi theo cách chia đôi"miền chưa biết" thì dãy các chữ số 0,1 thu được có biểu diễn số chưa biết trong hệ nhị phân không?

b) Cùng trong "trò chơi đoán số" giả sử được ghi một số từ 0 đến 1000; lúc đó, có thể hỏi không quá mấy câu thì biết được số phải tìm?

4.37 - *Trò chơi bốc diêm*

Trò chơi này được gọi là *trò chơi Nim*, đã được người Trung Quốc biết tới từ thời cổ xưa, "trò chơi với ba đống đá". Nay ta thay bằng "ba đống que diêm". - *Trò chơi bốc diêm*

Trước mặt hai bạn có ba đống que diêm, một đống có a = 3 que, một đống có b = 5 que và một đống có c = 7 que. Mỗi người thay phiên nhau bốc một que (tùy ý), nhưng mỗi lần đến lượt mình thì chỉ được bốc ở một đống thôi. Người nào bốc được que cuối cùng thì thắng.

Nếu biết cách chơi thì người đi trước chắc chắn thắng.

Hai bạn thử chơi với nhau và giải thích giùm. Nếu ba đống chứa 3,5,6 que thì sao? Tổng quát: với a,b,c bất kì thì sao?

■ 4. - Đại số mệnh đề với hệ nhị phân và máy tính

Năm 1854, khi nhà toán học Anh *G.Boole (Bun,* 1815-1864) cho ra đời cuốn sách "Các quy luật của tư duy" (còn được gọi là "đại số học của logic") thì không ai có thể nghĩ rằng một trăm năm sau, đại số Boole lại được phát triển rất mạnh mẽ và trở thành cơ sở lí thuyết của nhiều ngành kĩ thuật tính toán hiện đại.

Chúng ta hãy làm quen với phần mở đầu đơn giản của đại số Boole là *đại số mệnh đề*, và tìm hiểu mối liên hệ sâu xa với hệ ghi số nhị phân và máy tính.

4.1 - Đại số mệnh đề

Trong số học và đại số học, chúng ta làm các *phép toán* cộng và nhân trên các số. Mỗi phép toán cho ta một *quy tắc* để từ hai số cho trước ta có được một số thứ ba, gọi là kết quả của phép toán (tổng hoặc tích); quy tắc đó có thể cho bằng một bảng khi ta chỉ xét các số nhỏ hơn một số cho trước(thí dụ bảng nhân các số dưới 10). Các phép biến đổi đồng nhất trên các biểu thức đại số được thực hiện nhờ các tính chất cơ bản của phép cộng và phép nhân, như tính chất *giao hoán, kết hợp, tính chất phân phối của phép nhân đối với phép cộng.*

Bây giờ chúng ta hãy xét một tập hợp gồm các mệnh đề. Mệnh đề là một câu (viết hay nói) phản ánh một điều đúng hay sai.

Thí dụ về *mệnh đề đúng* :

- Quả đất quay quanh mặt trời.
- Tam giác ABC có một góc nhọn.

Thí dụ về *mệnh đề sai:*

- Mèo luôn đẻ ra trứng.
- 2 lớn hơn 3 ($2 > 3$).

Những câu sau đây không phải là mệnh đề (vì không thể nói là đúng hay sai được):

- Mèo có đẻ ra trứng không?
- Bạn hãy vẽ cho tôi một đường tròn!
- $x + 1 = 2$ (x cộng 1 bằng 2).

Ta sẽ chỉ mệnh đề bằng các chữ P,Q,R...

Nếu mệnh đề P là đúng thì ta nói:

P có trị đ, kí hiệu P = đ hay $P = 1$.

Nếu mệnh đề P là sai thì ta nói:

P có trị s, kí hiệu P = s hay $P = 0$.

Mỗi mệnh đề có một và chỉ một trong hai trị: đ(1) hoặc s(0). Người ta cũng gọi đ(1), s(0) là *trị chân lí* hay *chân trị* của mệnh đề.

Từ một hay nhiều mệnh đề, ta có thể lập những mệnh đề mới, bằng cách sử dụng các *liên từ*, biểu thị các *phép logic* (tương tự các phép toán trong đại số học). Sau đây ta xét ba phép logic cơ bản là: *phép phủ định, phép bội và phép tuyển.*

Phép phủ định

Với mọi mệnh đề P, ta có thể lập mệnh đề "*không phải P*"kí hiệu là $\overline{P}$ (hay P, P) và có *mệnh đề phủ định của P.*

Nếu P đúng (1) thì $\overline{P}$ sai (0)

Nếu P sai (0) thì $\overline{P}$ đúng (1)

Thí dụ:

P: 5 > 3 (đúng)

$\overline{P}$: *Không phải* 5 > 3 (sai)

P: tam giác ABC có hai góc vuông (sai)

$\overline{P}$: *không phải* tam giác ABC có hai góc vuông (đúng)

(Tam giác ABC *không có* hai góc vuông).

Định nghĩa trên đây của phép phủ định được ghi trong một bảng, gọi là *bảng phủ định.*

P	$\overline{P}$
0	1
1	0

Bảng phủ định

Phép hội

Cho hai mệnh đề:

P: Số π lớn hơn 2 ($\pi > 2$)

Q: Số π nhỏ hơn 4 ($\pi < 4$)

Ta có thể dùng từ nối "và" để ghép hai mệnh đề này lại, và được mệnh đề mới:

	Số $\pi > 2$	và	số $\pi < 4$.
	P	và	Q
Kí hiệu:	P	$\wedge$	Q
hay	P	&	Q

(đọc là: P và Q, hội của P,Q)

Dấu ∧ (&) được gọi là *dấu hội* hay *phép hội.*

Mệnh đề P ∧ Q có trị được xác định như sau:

P ∧ Q đúng khi và chỉ khi cả P lẫn Q đều đúng.

$$P \wedge Q = 1 \underset{\text{đn}}{\Leftrightarrow} P = Q = 1$$

Trong thí dụ trên, P đúng ($\pi > 2$ là đúng), Q cũng đúng ($\pi < 4$ là đúng) nên P ∧ Q đúng ($\pi > 2$ và $\pi < 4$, tức $2 < \pi < 4$ là đúng).

Nếu một trong hai mệnh đề P,Q là sai (hoặc cả P lẫn Q đều sai) thì P ∧ Q là sai. Thí dụ:

Số $\pi > 2$ và số $\pi < 3$ ($2 < \pi < 3$)

P∧Q

là sai, vì Q là sai ($\pi < 3$ là sai).

Định nghĩa của phép hội thường được ghi bằng một bảng, gọi là *bảng hội*.

P	Q	P∧Q
0	0	0
0	1	0
1	0	0
1	1	1

Bảng hội

Phép tuyển

Từ hai mệnh đề:

P: Số π lớn hơn 3

Q: Số π nhỏ hơn 2

Ta có thể lập mệnh đề mới:

Số π lớn hơn 3 *hoặc* số π nhỏ hơn 2

P *hoặc* Q

Kí hiệu: $P \vee Q$

(đọc là: P *hoặc* Q, P *hay là* Q, *tuyển của P và Q)*

Dấu $\vee$ được gọi là *dấu tuyển* hay *phép tuyển.*

Mệnh đề $P \vee Q$ có trị được xác định như sau:

$P \vee Q$ đúng khi và chỉ khi ít nhất một trong hai mệnh đề P,Q là đúng.

Nói cách khác:

$P \vee Q$ sai khi và chỉ khi cả P lẫn Q đều sai

$$P \vee Q = 0 \underset{\text{đn}}{\Leftrightarrow} P = Q = 0$$

Định nghĩa của phép tuyển có thể được cho bằng một bảng, gọi là *bảng tuyển.*

P	Q	P ∨ Q
0	0	0
0	1	1
1	0	1
1	1	1

Bảng tuyển

Thí dụ:

1) "$\pi > 3$ hoặc $\pi < 2$"

là đúng vì $\pi > 3$ đúng.

2) "$\pi > 2$ hoặc $\pi < 4$"

là đúng vì $\pi > 2$ đúng.

3) "$\pi < 2$ hoặc $\pi > 4$"

là sai vì cả "$\pi < 2$" lẫn "$\pi > 4$" đều sai.

Tính chất của các phép hội và tuyển

Dựa vào bảng hội, ta thấy rằng: hai mệnh đề $P \wedge Q$ và $Q \wedge P$ luôn luôn có cùng một trị, dù P, Q lấy trị gì. Người ta nói rằng $P \wedge Q$ *tương đương với* $Q \wedge P$ và viết:

$$P \wedge Q = Q \wedge P$$

Tương tự: $P \vee Q = Q \vee P$

nghĩa là *các phép hội và tuyển có tính chất giao hoán.*

Dựa vào các bảng hội và tuyển, ta cũng chứng minh được rằng: *phép hội và phép tuyển cũng có tính chất kết hợp; phép hội có tính phân phối đối với phép tuyển.*

1 là phần tử trung hòa của phép hội:

$$P \wedge 1 = 1 \wedge P = P$$

0 là phần tử trung hòa của phép tuyển:

$$P \vee 0 = 0 \vee P = P$$

Do các tính chất đó, ta có thể thực hiện các phép biến đổi tương đương trên các công thức, thành lập được từ các mệnh đề P,Q,R... nhờ các phép hội, tuyển và phủ định, tương tự như các phép biến đổi đồng nhất trong đại số, coi phép hội($\wedge$) như phép nhân (do đó thường viết P.Q hay PQ thay cho $P \wedge Q$), coi phép tuyển ($\vee$) như phép cộng.

(Chú ý rằng phép tuyển cũng có tính phân phối đối với phép hội, do đó trong các phép biến đổi tương đương cũng có thể coi phép tuyển ($\vee$) là phép nhân, phép hội ($\wedge$) là phép cộng).

Ta còn có:

$$P \wedge \overline{P} = 0$$

$$P \vee \overline{P} = 1$$

Tập hợp các mệnh đề, với các phép hội, tuyển, phủ định, có các tính chất cơ bản trên đây, được gọi là *đại số mệnh đề.*

Chú ý: Do tiếng Anh được sử dụng rộng rãi trong tin học, nên người ta thường nói:

- Mệnh đề có hai trị là t (*true*, nghĩa là *đúng*) và f (*false nghĩa là sai).*

Phép hội là phép *and* (nghĩa là *và).*

Phép tuyển là phép *or* (nghĩa là *hoặc).*

Phép phủ định là phép *no*(nghĩa là *không).*

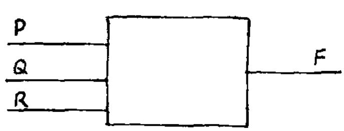
4.2 - Sơ lược về một ứng dụng vào máy tính điện tử

Đối với máy tính điện tử, mọi thông tin đều được biểu diễn dưới dạng mã số nhị phân, và trong kĩ thuật xử lí số liệu với mã số đó, đại số mệnh đề giữ vai trò rất quan trọng.

Ta sẽ tìm hiểu xem phép tính cộng hai số được thực hiện như thế nào.

Muốn vậy, ta chú ý đến các *phần tử logic cơ bản* trong máy tính. Đó là những chi tiết (các mạch tổ hợp) có một hoặc nhiều *đầu vào* P, Q, R...(mang tín hiệu vào) nhưng chỉ có một *đầu ra* F (mang tín hiệu ra) (h.1)

Hình 1



Ta sẽ viết:

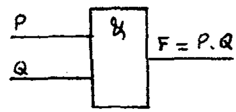
$$P = 1 \text{ khi P } \textit{có tín hiệu.}$$

$$P = 0 \text{ khi P } \textit{không có tín hiệu.}$$

Tương ứng với ba phép toán logic: hội, tuyển và phủ định, ta có ba phần tử logic cơ bản:

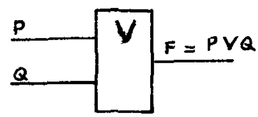
Phần tử **và (and)** thực hiện *phép hội (h. 2) : nó phát tín hiệu ra (F = 1) khi và chỉ khi ở tất cả các đầu vào đều có tín hiệu vào (P = Q = 1).*

Hình 2



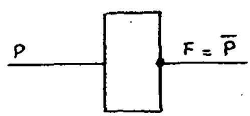
Phần tử **hoặc (or)** thực hiện phép tuyển (h. 3): nó phát tín hiệu ra (F = 1) khi và chỉ khi có tín hiệu vào ở ít nhất một đầu vào (P = 1 hoặc Q = 1)

Hình 3

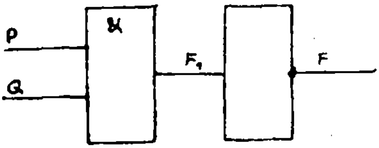


Phần tử **không (no)** thực hiện phép phủ định (h. 4) : chỉ có một đầu vào (P) và khi có tín hiệu vào (P = 1) thì nó không cho tín hiệu ra (F = 0) và ngược lại, khi không có tín hiệu vào (P = 0) thì nó phát tín hiệu ra (F = 1).

Hình 4



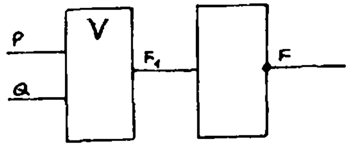
Có thể lắp ghép các phần tử logic cơ bản trên đây để được những mạch phức tạp hơn, lúc đó F cho ta công thức phức tạp hơn của P,Q. Các hình 5, 6, 7, 8 cho một số thí dụ.



$F_1 = P \,\&\, Q$

$F = \overline{F_1} = \overline{P \,\&\, Q}$

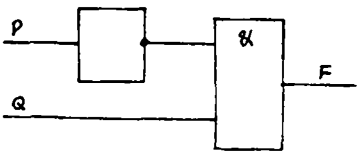
Hình 5



$F_1 = P \vee Q$

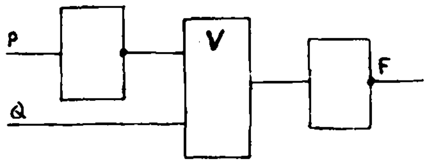
$F = \overline{F_1} = \overline{P \vee Q}$

Hình 6



$F = \overline{P} \,\&\, Q$

Hình 7



$F = \overline{\overline{P} \vee Q}$

Hình 8

Để xây dựng một mạch thực hiện phép cộng hai số có một chữ số trong hệ nhị phân, ta chú ý rằng tổng P + Q (trong đó P,Q là 0 hay 1) cho kết quả như sau:

$$0 + 0 = 00$$

$$0 + 1 = 01$$

$$1 + 0 = 01$$

$$1 + 1 = 10$$

Gọi chữ số đầu tiên (từ phải sang trái) của tổng là F_1, chữ số thứ hai là F_2, ta có bảng sau đây:

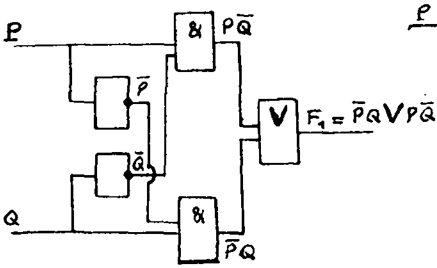
P	Q	F_2	F_1
0	0	0	0
0	1	0	1
1	0	0	1
1	1	1	0

Đối chiếu với bảng các phép logic cơ bản trong đại số mệnh đề, ta có:

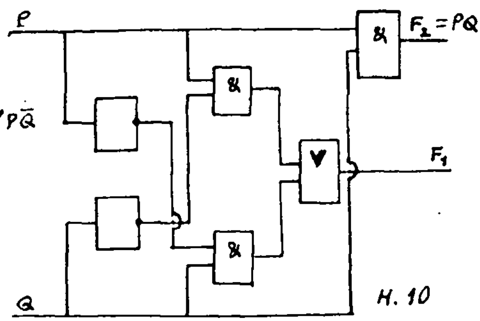
$$F_2 = P.Q \text{ (P và Q)}$$

$$F_1 = \overline{P}.Q \vee P.\overline{Q}$$

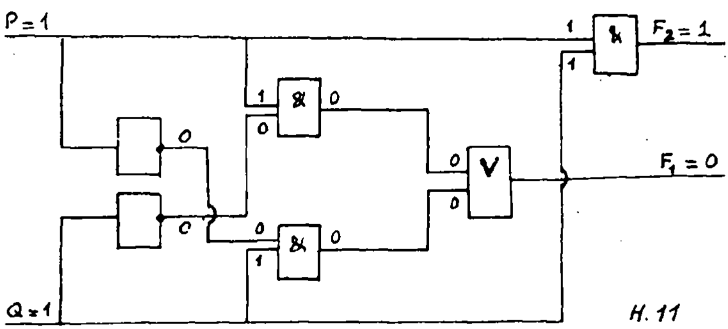
Hình 9 cho ta sơ đồ của F_1 và hình 10 cho ta sơ đồ của tổng P + Q (hình 11 cho sơ đồ tính tổng P + Q trong trường hợp P = Q = 1).



H. 9



H. 10



H. 11

PHỤ LỤC

LIÊN PHÂN SỐ

Liên phân số là một vấn đề rất hay của Số học, nhưng do khuôn khổ của cuốn sách này, chúng tôi chỉ giới thiệu một vài điều đơn giản nhất để sáng tỏ quy tắc đã nói ở chương III về giải phương trình Diophante bậc nhất (và phương trình đồng dư bậc nhất ở chương I).

1 - Lấy hai số tự nhiên tùy ý, chẳng hạn 162 và 47. Ap dụng *thuật toán Euclide* để tìm ƯCLN của chúng, ta có:

$$162 = 47.3 + 21$$

$$47 = 21.2 + 5$$

$$21 = 5.4 + 1$$

Như vậy: $(162, 47) = 1$

Bây giờ, ta viết các đẳng thức trên đây dưới dạng phân số:

$$\frac{162}{47} = 3 + \frac{21}{47} \qquad \text{(a)}$$

$$\frac{47}{21} = 2 + \frac{5}{21} \qquad \text{(b)}$$

$$\frac{21}{5} = 4 + \frac{1}{5} \qquad \text{(c)}$$

(a) có thể viết:

$$\frac{162}{47} = 3 + \cfrac{1}{\cfrac{47}{21}}$$

Thay $\frac{47}{21}$ theo (b), được:

$$\frac{162}{47} = 3 + \cfrac{1}{2 + \cfrac{5}{21}} = 3 + \cfrac{1}{2 + \cfrac{1}{\cfrac{21}{5}}}$$

Thay $\frac{21}{5}$ theo (c), được:

$$\frac{162}{47} = 3 + \cfrac{1}{2 + \cfrac{1}{4 + \cfrac{1}{5}}} \qquad \text{(d)}$$

Biểu thức ở vế phải của (d) được gọi là một *liên phân số (bậc 3).*

Tương tự như vậy, ta viết được $\frac{125}{54}$ dưới dạng liên phân số (bậc 4)như sau:

$$\frac{125}{54} = 2 + \cfrac{1}{3 + \cfrac{1}{5 + \cfrac{1}{1 + \cfrac{1}{2}}}}$$

Một cách tổng quát, có thể chứng minh rằng:

Mọi số hữu tỉ đều biểu diễn được một cách duy nhất dưới dạng một liên phân số bậc n:

$$\frac{a}{b} = q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \ddots + \cfrac{1}{q_n}}}$$

trong đó q_0 nguyên, q_1, q_2,..., q_n nguyên dương và $q_n > 1$.

Sau đây ta xét trường hợp $a > b > 0$, lúc đó q_0 cũng nguyên dương.

Liên phân số trên đây được kí hiệu là

$$[\, q_0;\, q_1,\, q_2, \ldots,\, q_n] \quad (1)$$

Thí dụ:

$$\frac{162}{47} = [\, 3;\, 2,\, 4,\, 5\,]$$

$$\frac{125}{54} = [\, 2;\, 3,\, 5,\, 1,\, 2\,]$$

2 - Ta gọi *giản phân bậc m* ($0 \le m \le n$) của liên phân số (1) là phân số $d_m = \dfrac{P_m}{Q_m}$ được xác định như sau:

Giản phân bậc 0:

$$d_0 = \frac{P_0}{Q_0} \quad \text{với} \quad P_0 = q_0 \quad \text{và } Q_0 = 1$$

Giản phân bậc 1:

$$d_1 = \frac{P_1}{Q_1} \quad \text{với} \quad P_1 = q_1 q_0 + 1$$

$$Q_1 = P_1$$

Giản phân bậc m (m = 2, 3,...n)

$$d_m = \frac{P_m}{Q_m} \quad \text{với} \quad P_m = q_m P_{m-1} + P_{m-2}$$

$$Q_m = q_m Q_{m-1} + Q_{m-2}$$

Ta thấy rằng:

$$'d_0 = \frac{P_0}{Q_0} = \frac{q_0}{1} = q_0$$

$$d_1 = \frac{P_1}{Q_1} = \frac{q_1 q_0 + 1}{q_1} = q_0 + \frac{1}{q_1} = [\, q_0 \,;\, q_1 \,]$$

$$d_2 = \frac{P_2}{Q_2} = \frac{q_2 P_1 + P_0}{q_2 Q_1 + Q_0} = \frac{q_2(\, q_1 q_0 + 1) + q_0}{q_2 q_1 + 1}$$

$$= q_0 + \frac{q_2}{q_2 q_1 + 1} = q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2}}$$

$$= [\, q_0;\, q_1,\, q_2]$$

Tổng quát, có thể chứng minh được rằng:

$$d_m = [q_0; \quad q_1, \quad q_2,\dots,q_m] \text{ với } 0 \le m \le n$$

và giản phân cuối cùng d_n là

$$d_n = [q_0;\, q_1,\, q_2,\dots,q_n]$$

Thí dụ:

$$[\, 3;\, 2,\, 4,\, 5] = 3 + \cfrac{1}{2 + \cfrac{1}{4 + \cfrac{1}{5}}}$$

có *giản phân bậc 0* là $d_0 = 3$

giản phân bậc 1 là $d_1 = [3; 2] = 3 + \frac{1}{2} = \frac{7}{2}$

giản phân bậc 2 là $d_2 = [3; 2, 4] = 3 + \cfrac{1}{2 + \cfrac{1}{4}} = \frac{31}{9}$

giản phân bậc 3 là $d_3 = [3; 2, 4, 5]$

(giản phân cuối cùng) $= 3 + \cfrac{1}{2 + \cfrac{1}{4 + \cfrac{1}{5}}} = \frac{162}{47}$.

3 - Ta chứng minh hệ thức rất quan trọng sau đây:

$$P_{m-1}Q_m - P_mQ_{m-1} = (-1)^m \qquad (2)$$

∇ Đặt $P_{m-1}Q_m - P_mQ_{m-1} = D_m \quad (1 \le m \le n)$

Theo công thức của P_m và Q_m trong định nghĩa của giản phân bậc m, ta viết được:

$$\begin{aligned} D_m &= P_{m-1}\,Q_m - P_m\,Q_{m-1} \\ &= P_{m-1}\,(q_mQ_{m-1} + Q_{m-2}) - (q_mP_{m-1} + P_{m-2})\,Q_{m-1} \\ &= -(P_{m-2}\,Q_{m-2} - P_{m-1}\,Q_{m-2}) \end{aligned}$$

$$D_m = -D_{m-1}$$

Mà $D_1 = P_0Q_1 - P_1Q_0 = q_1q_0 - (q_1q_0 + 1) = -1$

Do đó $D_2 = -D_1 = 1$, $D_3 = -D_2 = -1$, $D_4 = -D_3 = 1$.

Tổng quát là $D_m = (-1)^m$. □

Từ hệ thức (2) suy ra được rằng mọi ước chung của P_m và Q_m phải là ước của 1, nghĩa là P_m và Q_m nguyên tố cùng nhau, và *mọi giản phân đều là những phân số tối giản.*

Do đó, nếu $\frac{a}{b}$ là phân số tối giản (a,b nguyên tố cùng nhau), và $\frac{P_n}{Q_n}$ là giản phân cuối cùng biểu diễn nó, thì:

$$P_n = a \text{ và } Q_n = b.$$

4 - Áp dụng

4.1- Giải phương trình Diophante bậc nhất hai ẩn

Cho phương trình

$$ax + by = 1, \quad \text{với} \quad (a,b) = 1 \text{ và } b > 0.$$

Biểu diễn $\frac{a}{b}$ thành liên phân số, được:

$$\frac{a}{b} = [q_0 ; q_1, q_2, \ldots, q_n]$$

Giả sử $\frac{P_{n-1}}{Q_{n-1}}$ và $\frac{P_n}{Q_n}$ là hai giản phân cuối cùng của liên phân số này. Vì (a,b) = 1 và b > 0, nên có $P_n = a$ và $Q_n = b$.

Theo (2) thì

$$P_{n-1}Q_n - P_nQ_{n-1} = (-1)^n$$

do đó $\quad P_{n-1}\, b - a\, Q_{n-1} = (-1)^n$

hay là $\quad a(-1)Q_{n-1} + bP_{n-1} = (-1)^n$

Nhân hai vế với $(-1)^n$, được:

$$a.(-1)^{n-1}.Q_{n-1} + b.(-1)^nP_{n-1} = 1$$

tức là $\quad ax + by = 1$

có một nghiệm riêng là:

(3) $\quad x_0 = (-1)^{n-1}Q_{n-1}$

$$y_0 = (-1)^n P_{n-1}$$

Thí dụ: Giải phương trình

$$40x + 31y = 1$$

Ta có $(40, 31) = 1$

Dùng thuật toán Euclide, ta được:

$$40 = 31 \,.\, 1 + 9$$

$$31 = 9 \,.\, 3 + 4$$

$$9 = 4 \,.\, 2 + 1$$

Do đó

$$\frac{40}{31} = [\ 1;\ 3,\ 2,\ 4\ ]$$

Đây là một *liên phân số bậc 3*: $[\ q_0;\ q_1,\ q_2,\ q_3]$. Hai giản phân cuối cùng là $\frac{P_2}{Q_2}$ và $\frac{P_3}{Q_3} = \frac{40}{31}$

$$\frac{P_2}{Q_2} = [\ 1\ ;\ 3\ ,\ 2\ ] = \frac{9}{7}$$

tức là $P_2 = 9$, $Q_2 = 7$.

Áp dụng công thức (3) với $n = 3$, $n - 1 = 2$, ta có một nghiệm riêng của phương trình là:

$$x_0 = (-1)^2 .\ 7 = 7$$

$$y_0 = (-1)^3 .\ 9 = -9$$

Từ đó , có công thức của nghiệm tổng quát là:

$$x = 7 + 31t$$

$$y = -9 - 40t,\ t \in Z$$

4.2 - Giải phương trình đồng dư bậc nhất

Giải phương trình

$$ax \equiv b \quad (\text{mod } m)$$

với $(a,m) = 1$

Có thể giả thiết $1 < a < m$. Ta khai triển $\frac{m}{a}$ thành liên phân số:

$$\frac{m}{a} = [q_0; q_1, \ldots, q_n] = \frac{P_n}{Q_n}$$

$m = P_n$ và $a = Q_n$.

Theo (2) có

$$a P_{n-1} - m Q_{n-1} = (-1)^n$$

$$a P_{n-1} \equiv (-1)^n \ (\text{mod } m)$$

Nhân hai vế với $(-1)^n$. b, được:

$$a [(-1)^n b P_{n-1}] \equiv b \ (\text{mod } m)$$

Vậy phương trình có nghiệm là

$$x \equiv (-1)^n b P_{n-1} \ (\text{mod } m)$$

Thí dụ: Giải phương trình

$$7x \equiv 3 \quad (\text{mod } 27)$$

$m = 27, a = 7, \qquad (27, 7) = 1.$

$27 = 7.\ 3 + 6$

$7 = 6.\ 1 + 1$

Vậy $\frac{27}{7} = [3; 1, 6] = \frac{P_n}{Q_n}, \ n = 2$

$$\frac{P_{n-1}}{Q_{n-1}} = [3; 1] = \frac{4}{1}, \ P_{n-1} = 4$$

Do đó

$$x \equiv (-1)^n b P_{n-1} = 3 \ .\ 4 = 12 \quad (\text{mod } 27)$$

5 - *Liên phân số có nhiều ứng dụng khác nữa*; sau đây là một vài thí dụ:

Người ta chứng minh được rằng: mọi số vô tỉ, nếu là căn bậc hai của các số không chính phương thì có thể biểu diễn dưới dạng *liên phân số vô hạn tuần hoàn*, chẳng hạn:

$$\sqrt{3} = 1 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{2 + \ldots}}}} = [\ 1;\ 1,\ 2,\ 1,\ 2, \ldots]$$

Người ta kí hiệu:

$$\sqrt{3} = [\ 1;\ 1,2\ ]$$

Tương tự:

$$\sqrt{2} = [1;\ 2\ ]$$

$$\sqrt{5} = [\ 2;\ 4\ ]$$

$$\sqrt{6} = [\ 2;\ 2,4\ ]$$

Việc giải *phương trình Pell* (xem chương III) dựa vào kết quả này.

- Từ thời cổ Hi Lạp, người ta đã quan tâm đến phép chia một đoạn thẳng AC ra hai phần AB = a và BC = b sao cho:

$$\frac{a}{b} = \frac{a+b}{a}$$

Lấy b = 1, có

$$a = \frac{a+1}{a} \qquad \text{hay } a^2 - a - 1 = 0$$

do đó

$$a = \frac{1+\sqrt{5}}{2}$$

Giá trị này của a có thể viết dưới dạng *liên vô hạn tuần hoàn:*

$$a = \frac{1+\sqrt{5}}{2} = 1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \dots}}} = [\,1, 1\,]$$

Phép chia theo tỉ lệ a như trên được gọi là " *phép chia vàng*", đã có lúc được gọi là phép chia " đẹp" nhất, nhiều công trình kiến trúc có kích thước một số bộ phận theo tỉ lệ a.

- Trong *thiên văn học*, người ta tìm thấy rằng quả đất quay một vòng quanh mặt trời mất 365 ngày 5 giờ 48 phút 46 giây, số ngày này viết ra dưới dạng liên phân số là

$$[\,365;\ 4,7,1,3,5,20,6,12\,]$$

Nếu lấy một năm là 365 ngày, rồi cứ 4 năm một lần có một năm nhuận (thêm một ngày) thì số ngày trong năm tương ứng với giản phân bậc I của liên phân số trên:

$$[\,365;\ 4\,] = 365 + \frac{1}{4} = 365\frac{1}{4}$$

Các giản phân tiếp theo cho kết quả chính xác hơn:

$$[\,365;\ 4,7\,] = 365 + \cfrac{1}{4 + \cfrac{1}{7}} = 365\frac{7}{29}$$

(29 năm chứ không phải 28 năm, có 7 năm nhuận).

$$[\,365;\ 4,7,1\,] = 365\frac{8}{33}$$

(33 năm chứ không phải 32 năm, có 8 năm nhuận).

$$[\,365;\ 4,7,1,3] = 365\frac{31}{128}$$

(128 năm mới có 31 năm nhuận chứ không phải 32 năm nhuận).

GỢI Ý

GIẢI MỘT SỐ BÀI TẬP

1.2 Trong k số tự nhiên liên tiếp, bao giờ cũng có một số chia chia hết cho k.

a) Trong ba số n, n + 1, n + 2 có một số chia hết cho 3 và một số chia hết cho 2, mà (3,2) = 1, nên tích ba số đó chia hết cho 2.3 = 6.

Trong bốn số n, n + 1 , n + 2, n + 3 có một số chia hết cho 4, một số chia hết cho 2 (hai số này khác nhau), nên tích bốn số chia hết cho 2.4 = 8. Tích cũng chia hết cho 3, mà (3,8) = 1 nên tích chia hết cho 3.8 = 24.

b) (24,5) = 1, tích chia hết cho 24.5 = 2.3.4.5 = 120.

c) $2k(2k + 2) = 4k(k + 1) \vdots 8$, vì $k(k + 1) \vdots 2$

d) $2k(2k + 2)(2k + 4) = 8k(k + 1)(k + 2) \vdots 8.6 = 48$

1.3 $A = n^2(n^2 - 1) = (n - 1)n^2(n + 1)$

$(n - 1)n(n + 1) \vdots 3 \Rightarrow A \vdots 3$

n chẵn $\Rightarrow n^2 \vdots 4 \Rightarrow A \vdots 4$

n lẻ $\Rightarrow (n - 1)(n + 1) \vdots 4 \Rightarrow A \vdots 4$

$(3,4) = 1 \Rightarrow A \vdots 3.4 = 12$

1.4 $120 = 2^3.3.5$, $A(n) \vdots 5$ với mọi n (thí dụ 1, trang 15)

n chẵn $\Rightarrow n^2 + 4 \vdots 4 \Rightarrow A(n) \vdots 8 = 2^3$

$n \vdots 3 \Rightarrow A(n) \vdots 3$

n lẻ hoặc $n \not\vdots 3$ thì không có các tính chất trên.

Vậy $n \vdots 2.3 = 6$

1.5 $A(n) \vdots 12$ (bài 1.3)

$A(n) \vdots 5$ với mọi n : $n = 5k \pm 1 \Rightarrow (n - 1)(n + 1) \vdots 5$

$n = 5k \pm 2 \Rightarrow n^2 + 1 \vdots 5$

1.6 a) $(n + 1)(n + 3)$ là tích hai số chẵn liên tiếp

hoặc $(2k + 1)^2 + 4(2k + 1) + 3 = 4(k^2 + 3k + 2)$

mà $k^2 + 3k + 2 = k(k + 3) + 2 \vdots 2$

b) $A(n) = (n - 1)(n + 1)(n + 3)$, tích của ba số chẵn liên tiếp.

Hoặc dùng qui nạp toán học. Giả sử $A(k)$ đúng, chứng minh

$A(k + 2)$ đúng (k lẻ, số lẻ tiếp sau là $k + 2$)

$A(k + 2) = A(k) + 6(k^2 + 4k + 3)$, trở lại 1.6a.

1.7 Có thể dùng qui nạp toán học:

a) $4^{k+1} + 15(k + 1) - 1 = (4^k + 15k - 1) + 3(4^k + 5)$

$$4^k = 3M + 1$$

b) $A(k + 1) = A(k) + 9(10^k + 2)$, $10^k = 9Q + 1$

1.8 a) $(2k + 1)^2 = 4k^2 + 4k + 1 = 4k(k + 1)$; $k(k + 1) \vdots 2$

b) $2^{1000} = (2^2)^{500} = (5 - 1)^{500}$, số dư là 1.

c) $25 = 5.5$, $2^{1000} = 2^{500} . 2^{500} = (5 - 1)^{250} . (5 - 1)^{250}$

1.9 $A(n) = n(n + 1)(n + 2)(n + 3)$, trở lại bài 1.2a

Hoặc dùng qui nạp toán học

$A(k) = k^4 + 6k^3 + 11k^2 + 6k \Rightarrow A(k + 1) = A(k) +$
$24(k^2 + 1) + 4(k^3 + 11k)$

$k^3 + 11k = k(k^2 + 11) = k(k^2 - 1 + 12) = k(k^2 - 1) + 12k$

$= (k - 1)k(k + 1) + 12k : 6$

(hoặc chứng minh $k^3 + 11k : 6$ bằng qui nạp toán học)

1.10 – $384 = 2^7.3$, $A(n) = A(2k) = 2^4.k(k^3 - 2k^2 - k + 2)$

$k^3 - 2k^2 - k + 2 = k^2(k - 2) - (k - 2)$

$= (k - 2)(k - 1)k(k + 1) \vdots 24 = 2^3.3$

1.11 – Xem 4 – Định lý Fermat và định lý Euler, trang 38.

1.12 a) $A(n) = n^4 - 1 = (n-1)(n+1)(n^2+1) \vdots 8 \Leftrightarrow n \vdots 2$

(lúc đó $n - 1$, $n + 1$ và $n^2 + 1$ đều chẵn)

b) $n^6 - 1 = (n^3 - 1)(n^3 + 1)$, $n \vdots 3 \Rightarrow n^3 - 1$ và $n^3 + 1 \vdots 3$

1.13 $(n,6) = 1 \Rightarrow (n,2) = (n,3) = 1$

$(n,2) = 1 \Rightarrow (n-1)(n+1) \vdots 8$ (tích hai số chẵn liên tiếp)

$(n,3) = 1 \Rightarrow (n-1)(n+1) \vdots 3$

1.14 $3^{6n} - 2^{6n} = (3^3)^{2n} - (2^3)^{2n} = (27 + 8)P$

1.15 $30 = 6.5$

$ab(a^2 - b^2) \vdots 6$ vì $ab(a^2 - b^2) = ab(a^2 - 1) - ab(b^2 - 1)$

$= b(a-1)a(a+1) - a(b-1)b(b+1)$

mà $(a-1)a(a+1)$, $(b-1)b(b+1)$ đều $\vdots 6$

$ab(a^2 - b^2)(a^2 + b^2) \vdots 5$. Xét mọi trường hợp: a hoặc b chia hết cho 5; giá trị tuyệt đối của số dư khi chia a và b cho 5 là bằng nhau (lúc đó $a^2 - b^2 \vdots 5$), giá trị tuyệt đối của số dư đó khác nhau (lúc đó $a^2 + b^2 \vdots 5$)

1.16 a) Đặt $m = 3p \pm r$ $(r = 0,1)$, $n = 3q \pm s$ $(s = 0,1)$

$m^2 + n^2 \vdots 3 \Leftrightarrow r^2 + s^2 \vdots 3$ $(0 \le r^2 + s^2 \le 2) \Leftrightarrow r = s = 0$

b) Đặt $m = 3p \pm r$ $(r = 0,1,2,3)$, $n = 3q \pm s$ $(s = 0,1,2,3)$

c) $m^2 + n^2 = (m^2 - 4n^2) + 5n^2 \vdots 5$

Có thể xét mọi trường hợp về số dư khi chia m và n cho 5.

Cách khác:

$m^2 - 4n^2 = (m + 2n)(m - 2n) \vdots 5 \Rightarrow 2n + m \vdots 5$ hoặc $2n - m \vdots 5$

$2n + m \vdots 5 \Rightarrow 2n - 4m + 5m = 2(n - 2m) + 5m \vdots 5$

$\Rightarrow 2m - n \vdots 5$

$2n - m \vdots 5 \Rightarrow 2n + 4m - 5m = 2(n + 2m) - 5m \vdots 5$

$\Rightarrow 2m + n \vdots 5$

d) $m^3 + n^3 = (m^3 - m) + (n^3 - n) + (m + n)$

$= (m-1)m(m+1) + (n-1)n(n+1) + (m+n)$

$m^3 + n^3 \vdots 6 \Leftrightarrow m + n \vdots 6$

1.17 Biến đổi thành $3a(a + 1) + 6 + (a^2 - 1)$

$$a^2 - 1 = (a - 1)(a + 1) \vdots 6 \Leftrightarrow (a, 6) = 1$$

1.18 $A(n) = n^2(n^6 - n^4 - n^2 + 1) = n^2(n^4 - 1)(n^2 - 1)$

$= [n(n^2 - 1)]^2 . (n^2 + 1)$

$A(2k + 1) = [(2k + 1)(4k^2 + 4k)]^2 . (4k^2 + 4k + 2)$

$= 32[(2k + 1)k(k + 1)]^2 . (2k^2 + 2k + 1)$

Mà $(2k + 1)k(k + 1) \vdots 6$, do trong ba thừa số của nó bao giờ cũng có một số chẵn và một bội của 3.

$$\Rightarrow A(2k + 1) \vdots 32.36 = 1152.$$

1.19 a) và b) Chia một số cho m, các số dư là một trong m số từ 0 đến m – 1. Chia m + 1 số cho m, phải có ít nhất hai số cho cùng số dư, hai số này có hiệu chia hết cho m (m = 10 thì hai số đó có cùng chữ số sau cùng).

c) Gọi các số đã cho là $a_1, a_2, a_3, ..., a_m$. Lập m tổng:

a_1

$a_1 + a_2$

$a_1 + a_2 + a_3$

...

$a_1 + a_2 + ... + a_m$

Có hai trường hợp:

– Một trong các tổng trên chia hết cho m;

– Không có một tổng nào chia hết cho m; thế thì tìm được hai tổng cho cùng số dư khi chia cho m (vì có m tổng mà chỉ có m – 1 số dư). Hiệu của chúng (là một tổng của các số đã cho) chia hết cho m.

d) Chia 5 số nguyên cho 3 thì hoặc có 3 số cho cùng số dư, hoặc có 3 số cho số dư đôi một khác nhau; trong mọi trường hợp, tổng của 3 số này chia hết cho 3.

1.20 – Lập 1990 số có dạng

1991

1991 1991

1991 1991 1991

...

1991 1991 ... 1991 (1990 lần 1991)

Chia các số đó cho 1990, có *1989 số dư khác 0*. Theo nguyên tắc Dirichlet, phải có ít nhất hai số cho cùng một số dư; hiệu của hai số đó (có dạng 1991 1991 ... 0000) chia hết cho 1990.

1.21 – a) $(n-2)^2 + (n-1)^2 + n^2 + (n+1)^2 + (n+2)^2 = 5(n^2+2)$ mà $n^2 + 2 \not\vdots\, 5$

b) Trong ba số nguyên liên tiếp, có một số là bội của 3, hai số kia có dạng $3p \pm 1$. Mà $(3p \pm 1)^{2k} = 3.P + 1$, nên tổng các lũy thừa chẵn của ba số nguyên liên tiếp có dạng $3Q + 2$. Nhưng lũy thừa chẵn của một số n chỉ có thể có dạng 3M (khi n là bội của 3) hoặc $3P + 1$ (khi n có dạng $3p \pm 1$).

1.22 b) $A(n) = n^2 + 11n + 18) + 21 = (n+9)(n+2) + 21$

Mà $(n+9) - (n+2) = 7$, nên $n+9$ và $n+2$ cùng chia hết cho 7 (lúc đó $(n+9)(n+2) \vdots 49$, trong khi $21 \not\vdots\, 49$, do đó $A(n) \not\vdots\, 49$;

hoặc $n+9$ và $n+2$ đều không chia hết cho 7 (lúc đó

$(n+9)(n+2) \not\vdots\, 7$, trong khi $21 \vdots 7$, do đó $A(n) \not\vdots\, 7$, tức $A(n) \not\vdots\, 49$

c) $n^2 + 3n + 5 = (n+7)(n-4) + 33$, mà

$(n+7) - (n-4) \vdots 11$. Tương tự b)

1.23 $\overline{ab} \vdots 7 \Rightarrow 10a + b \vdots 7 \Rightarrow 3a + b \vdots 7 \Rightarrow b = 7k - 3a$

$a^3 - b^3 = a^3 - (7k - 3a)^3 \vdots 7$.

1.24 Gọi tích đã cho là P. Ta chứng minh $P \vdots 3$ và $P \vdots 4$. Trong *bốn số a, b, c, d* bao giờ cũng có hai số mà hiệu chia hết cho 3 (bài 1.19b), do đó $P \vdots 3$.

Trong bốn số a, b, c, d nếu có hai số chẵn và hai số kia lẻ thì hiệu của hai số chẵn cũng như hiệu của hai số lẻ đều chia hết cho 2, do đó $P \vdots 4$. nếu có ba số (thí dụ *a, b, c*) là số chẵn hoặc số lẻ thì $b - a$, $c - a$ chia hết cho 2 và $P \vdots 4$.

1.25 $(a + b + c)^3 - (a^3 + b^3 + c^3) = 3(b + c)(a + b)(a + c)$

mà $b + c$, $a + b$, $a + c$ đều là bội của 2.

1.26 $1^3 + 7^3 = (1 + 7).M$, $3^3 + 5^3 = (3 + 5).N$

1.27. $a^3 - b^3 = (a - b)(a^2 + ab + b^2)$. Do a và b là số lẻ, nên

$(a^2 + ab + b^2, 2^n) = 1$

1.28 $((2k - 1)^2 - 1)((2k + 1)^2 + 1) = 16k^2(k - 1)(k + 1)$

mà $k^2(k - 1)(k + 1) \vdots 12$ (bài 1.3)

1.29 $- 3(3^0 + 3^2) + 3^5(3^0 + 3^2) + ...+ 2^{2n-3}(3^0 + 3^2)$

$= 3.10(1 + 3^4 + ...+ 3^{2n-4}) \vdots 30$

1.30 $12^{2n+1} + 11^{n+2} = 144^n . 12 + 11^n . 121$

$= 12(144^n - 11^n) + 12.11^n + 121.11^n = 12.133M + 133.11^n$

Có thể dùng qui nạp toán học.

1.31 a) $n^2 + 1 = (n + 1)^2 - 2(n + 1) + 2 \vdots n + 1$

$\Leftrightarrow 2 \vdots n + 1$ tức $n = 1$

b) $n^2 + 2n + 6 = (n + 4)^2 - 6(n + 4) + 14 \vdots n + 4$

$\Leftrightarrow 14 \vdots n + 4 \Leftrightarrow n = 3,10.$

1.32 $(n + 5)(n + 6) = 12n + (n^2 - n + 30) \vdots 6n$

$\Leftrightarrow n^2 - n + 30 = n(n - 1) + 30 \vdots 6n$

Vì $n(n - 1) \vdots n$ nên phải có $30 \vdots n$, đồng thời vì $30 \vdots 6$, nên phải có $n(n - 1) \vdots 6$. Do $n(n - 1)$ luôn là bội của 2,

$n(n - 1) \vdots 6 \Leftrightarrow n(n - 1) \vdots 3$, tức $n = 3k$ hoặc $3k + 1$.

Tóm lại, n phải là ước của 30 và có dạng 3k hoặc 3k + 1:

$n = 1, 3, 10, 30.$

1.33 Chú ý rằng $a^4 - 1 \vdots 5$ với $a = 1, 2, 3, 4$.

$a^{4k} - 1 = (a^4 - 1). M \vdots 5 \Rightarrow a^{4k} = 5A + 1$

$n = 4k + r \ (r = 0, 1, 2, 3) \Rightarrow a^n = a^{4k}. a^r = (5A + 1) . a^r$

Như vậy, chia a^n cho 5 thì số dư là a^r

$\Rightarrow$ Chia $1^n + 2^n + 3^n + 4^n$ cho 5, có dư là $1 + 2^r + 3^r + 4^r$

$P(n) = 1^n + 2^n + 3^n + 4^n \vdots 5 \Leftrightarrow P(r) = 1 + 2^r + 3^r + 4^r \vdots 5$

$P(0) = 4 \not\vdots 5$, $P(1) = 10$, $P(2) = 30$, $P(3) = 100$ đều $\vdots\ 5$

1.34 Chú ý rằng $1 + 2 + ... + (n - 1) + n = n(n + 1) / 2$, ta chứng minh $P = 1 + 2^k + ... + (n - 1)^k + n^k \vdots n(n + 1) / 2$.

Với k lẻ và n chẵn $(n = 2m)$ thì $1 + n^k : 1 + n, ...,$

$2^k + (n - 1)^k : 2 + (n - 1) = n + 1$

$\Rightarrow P \vdots n + 1$

Mặt khác, $(2m)^k \vdots m$, $1 + (2m - 1)^k \vdots m$, ..., $m^k \vdots m$

$\Rightarrow P \vdots m$

Tương tự với k lẻ và n lẻ.

1.35 Số b phải chẵn, và chỉ cần xét $b = 2, 4, 8$ ($b = 6$: hiển nhiên)

$2^n - b = 10a : 10 \Rightarrow 2^n$ tận cùng là $b = 2, 4, 8$

hay 2^n tận cùng là $b = 2^r$ $(r = 1, 2, 3)$

Chú ý rằng nếu p là một lũy thừa của 2 thì b.p có tận cùng là b khi và chỉ khi $p = 2^{4k}$($2^4 = 16$) và $2 \times 16 = 32$, $4 \times 16 = 64$, $8 \times 16 = 128$)

Do đó

2^n tận cùng là 2^r $(r = 1, 2, 3) \Leftrightarrow n = 4k + r$

$2^n - b = 2^{4k+r} = 2^r(2^{4k} - 1) = 2^r(16^k - 1) = 2^r.15.M \vdots 30$

$2^n - b = 10a \vdots 30 \Rightarrow a : 3 \Rightarrow a.b \vdots 6$

Có thể dùng *qui nạp toán học:*

Gọi mệnh đề phải chứng minh là A(n)

Thử trực tiếp, có A(4), A(5) đúng.

Giả sử A(k − 1) và A(k) đúng, ta chứng minh A(k + 1) đúng, tức là $2^{k+1} = 10a_{k+1} + b_{k+1}$ $(b_{k+1} < 10) \Rightarrow a_{k+1} \cdot b_{k+1} \vdots 6$

Thực vậy:

$2^k = 10a_k + b_k$ (giả thiết) $\Rightarrow b_k$ chẵn.

$2^{k+1} = (10a_k + b_k).2 = 10a_{k+1} + b_{k+1}$

$b_k \leq 4 \Rightarrow a_{k+1} = 2a_k$, $b_{k+1} = 2b_k$

$\Rightarrow a_{k+1} \cdot b_{k+1} = 4a_kb_k \vdots 6$

$b_k = 8 \Rightarrow b_{k+1} = 6 \Rightarrow a_{k+1} b_{k+1} \vdots 6$

$b_k = 6 \Rightarrow a_{k+1} = 2a_k + 1, b_{k+1} = 2$

Mà $b_k = 6$ thì $b_{k-1} = 8$ và $a_{k-1}, b_{k-1} \vdots 6$ (giả thiết)

$\Rightarrow a_{k-1} = 3p$ và $a_k = 2a_{k-1} + 1 = 6p + 1$

$\Rightarrow a_{k+1} = 2a_k + 1 = 12p + 3 \vdots 3 \Rightarrow a_{k+1} . b_{k+1} \vdots 6$

1.36 $a_n - b_n = 2.2^{n+1} = 2^{n+2} \vdots 5 \Rightarrow a_n$ và b_n không cùng $\vdots 5$

$a_n . b_n = 2 . 2^{2(n+1)} + 1 = 4^{2n+1} + 1 \vdots 5 \Rightarrow a_n$ hoặc $b_n \vdots 5$

Cách khác: Viết $n = 4k + r$ ($r = 0,1,2,3$) và xét mọi trường hợp với r.

1.37 $2^3 = 8 = 7 + 1$, $n = 3k + r$ ($r = 0, 1, 2$)

$\Rightarrow 2^n = 2^{3k+r} = 2^{3k}.2^r = (7 + 1)^k . 2^r$

$2^n - 1 \vdots 7$ khi và chỉ khi $r = 0$, tức $n = 3k$

$2^n + 1 \not\vdots 7$ với mọi $r = 0, 1, 2$ (tức là với mọi n)

1.38 a) $11^{10} - 1 = (11 - 1)(11^9 + 11^8 + ... + 11 + 1) = 10B$ mà B là tổng của 10 số hạng, mỗi số hạng tận cùng là 1, nên $B \vdots 10$

b) $2222^{5555} + 5555^{2222} = (2222^{5555} + 4^{5555}) + (5555^{2222} - 4^{2222}) - (4^{5555} - 4^{2222}) = A + B - C$

$A \vdots 2222 + 4 = 7.318$, $B \vdots 5555 - 4 = 7.783$

$C = 4^{2222}(4^{3333} - 1) = 4^{2222}(64^{1111} - 1) \vdots 63 = 7.9$

1.39 Chứng minh bằng quy nạp:

Giả sử có k số đôi một nguyên tố cùng nhau:

$a_1 = 2^{n_1} - 3, a_2 = 2^{n_2} - 3 ... a_k = 2^{n_k} - 3$ trong đó:

$2 = n_1 < n_2 < ... < n_k$. Ta tìm được số $a_{k+1} = 2^{n_{k+1}} - 3$ nguyên tố với tất cả k số ở trên.

Đặt $m = a_1 . a_2 ... a_k \Rightarrow$ trong $m + 1$ số $2^0, 2^1, ..., 2^m$ có hai số 2^r và 2^s mà hiệu chia hết cho m (bài 1.19b)

$$2^r - 2^s = 2^s(2^{r-s} - 1) \vdots m \ (r > s)$$

$$(2,m) = 1 \Rightarrow 2^{r-s} - 1 \vdots m \text{ hay } 2^{r-s} - 1 = mt$$

Ta lấy $a_{k+1} = 2^{r-s+2} - 3 \ (= 4mt + 1 > a_k)$

$\Rightarrow (a_{k+1}, m) = 1 \Rightarrow a_{k+1}$ nguyên tố với $a_1, a_2, \dots, a_k$

Tiếp tục quá trình trên đây, ta có vô số các số có dạng $2^n - 3$ đôi một nguyên tố cùng nhau.

1.40 a) $72 = 9.8$, $3^n + 63 \vdots 9 \Leftrightarrow n \geq 2$

$$3^n + 63 = 3^n - 1 + 64 \vdots 8 \Leftrightarrow 3^n - 1 \vdots 8 \Leftrightarrow n \text{ chẵn.}$$

Vậy $\quad n = 2k, \ k \geq 1$

b) $323 = 17.19$

$$A(n) = (20^n - 1) + (16^n - 3^n) = P + Q$$

$P \vdots 19$, còn $Q = (16 + 3) M \vdots 19$ nếu *n chẵn.*

$$A(n) = (20^n - 3^n) + (16^n - 1) = P' + Q'$$

$P' \vdots 17$, còn $Q' = (16 + 1).M' \vdots 17$ nếu *n chẵn.*

Kết luận: $A(n) \vdots 17.19$ nếu *n chẵn.*

1.41 Từ thuật toán Euclide để tìm UCLN

1.43 a) Bất cứ số nào là ước chung của a va b cũng là ước chung của a và $a \pm b$; và ngược lại.

b) $(ab, c) = d > 1 \Rightarrow c \vdots p$ và a (hoặc b) $\vdots$ p (với p à một thừa số nguyên tố của d) $\Rightarrow$ p là ước chung của c và a (hoặc của c và b), trái với giả thiết.

c) Áp dụng a) và b)

$$(a, b) = 1 \Rightarrow (a, a \pm b) = 1$$

$$(b, a \pm b) = 1$$

$$\Rightarrow (ab, a \pm b) = 1$$

1.44 $a^4 + 3a^2 + 1 = (a^3 + 2a) \,.\, a + (a^2 + 1)$

$$a^3 + 2a = (a^2 + 1).a + a$$

$$a^2 + 1 = a.a + 1$$

1.45 a) $n + 13 = (n - 2) + 15$

$$(n - 2, 15) = 1 \Leftrightarrow \begin{cases} n - 2 \neq 3t \\ n - 2 \neq 5k \end{cases}$$

b) $\dfrac{18n + 3}{21n + 7} = \dfrac{3(6n + 1)}{7(3n + 1)}$

Đã có $(3,7) = (3, 3n + 1) = (6n + 1, 3n + 1) = 1$, còn phải có $(6n + 1, 7) = 1$

$6n + 1 = 7n - (n - 1) \Rightarrow (6n + 1, 7) = 1 \Leftrightarrow (n - 1, 7) = 1$

$$\Leftrightarrow n \neq 7t + 1$$

c) $6n + 5 = (5n + 6) + n - 1$

$5n + 6 = (n - 1)5 + 11$

$(6n + 5, 5n + 6) = (n - 1, 11) = 1 \Leftrightarrow n \neq 11t + 1$

1.46 Dùng thuật toán Euclide.

1.47 Dùng thuật toán Euclide, đi tới:

$d = (18a + 5b, 11a + 2b) = (a - 5b , 19b)$

$d \mid 19b \Rightarrow d \mid b$ hoặc $d \mid 19$

$d \mid b \Rightarrow d \mid a$ (do $d \mid a - 5b$) $\Rightarrow d = 1$, do $(a, b) = 1$

$d \mid 19 \Rightarrow d = 19$ hoặc $d = 1$

1.48 a) $(n, n + 2) = d \Rightarrow n \vdots d$ và $n + 2 \vdots d$

$$\Rightarrow 2 \vdots d \Rightarrow d = 1 \text{ hoặc } d = 2$$

b) $(n, n + 1) = 1$

1.49 $[a, b, c] = [[a, b], c]$

$m = [n, n + 1, n + 2] = [[n, n + 1], n + 2]$

mà $[n, n + 1] = n(n + 1)$

$\Rightarrow m = [n(n + 1), n + 2] = n(n + 1)(n + 2)$ nếu n lẻ

$= \dfrac{1}{2} n(n + 1)(n + 2)$ nếu n chẵn.

1.50 a) Ước chung của hai số a và a + m phải là ước của m. Với 5 số nguyên dương liên tiếp thì $0 < m \leq 4 \Rightarrow d = (a, a + m) \leq 4$

Trong 5 số nguyên dương liên tiếp, có ít nhất hai số lẻ liên tiếp, trong hai số lẻ này ít nhất một số không chia hết cho 3 và một số lẻ không chia kết cho 3 thì không thể có ước chung là 2, 3, 4 với bốn số kia, nghĩa là phải nguyên tố với chúng.

151 a) a và b đều chia hết cho 9; $a + 10b = 9999999999 = 10^{10} - 1$

$a + b = 1111111110 \Rightarrow 9a + 9b = 10^{10} - 10$

$b - 8a = 9 \Rightarrow (a, b) = 9$

b) $[a, b] = \frac{ab}{(a, b)} = \frac{ab}{9} \frac{a}{9} = 13717421 = 11.p + 3$

$b = 11q + 5 \Rightarrow \frac{ab}{9} = (11p + 3)(11q + 5) = 11.M + 15$

[a, b] chia cho 11, dư 4.

1.52 $d = (m + n , m^2 + n^2) \Rightarrow (m + n)^2 \vdots d \Rightarrow (m + n)^2 -$

$(m^2 + n^2) = 2mn \vdots d \Rightarrow d$ là ước chung của $m + n$ và $2mn$. (a)

$(m, n) = 1 \Rightarrow (m + n, n) = (m + n, m) =$

$(m + n, mn) = 1$ (b)

Do (a) và (b) $\Rightarrow 2 \vdots d \Rightarrow d = 1$ hoặc $d = 2$.

1.53 $d = (a, c) \Rightarrow a = a_1d, c = c_1d$ với $(a_1, c_1) = 1$ (1)

$ab = c^n \Rightarrow a_1db = (c_1d)^n$

$a_1b = d^{n-1} . C_1^n$ (2) $\Rightarrow d^{n-1} . c_1^n \vdots b$

$\Rightarrow c_1^n \vdots b$ (3)

Mà $(d, b) = (a, b) = 1 \Rightarrow (d^{n-1} , b) = 1$

(1) $\Rightarrow (a_1, c_1^n) = 1$

(2) $\Rightarrow a_1b \vdots c_1^n$

$\Rightarrow b \vdots c_1^n$ (4)

(3) và (4) $\Rightarrow c_1^n = b$, và (2) $\Rightarrow d_1^n = a_1 \Rightarrow d^n = a$

Lấy $p = d$, $q = c_1$, sẽ có $p^n = d^n = a$, $q^n = c_1^n = b$

và $(p, q) = (d, c_1) = 1$.

1.54 a) Suy từ $\min(a, b) + \max(a, b) = a + b$, với mọi a, b.

b) Không mất tính tổng quát, có thể giả sử $p \leq q \leq r$

$\min(q, r) = q$, $A = \max(p, \min(q, r)) = \max(p, q) = q$

$\max(p, q) = q$ $\max(p, r) = r$

$\Rightarrow B = \min(\max(p, q), \max(p, r)) = \min(q, r) = q$

$\Rightarrow A = B$

Áp dụng: Giả sử khi phân tích *a, b, c* ra thừa số nguyên tố, mỗi thừa số p_i có số mũ là a_i trong a, b_i trong b và c_i trong c.

Thế thì thừa số p_i có số mũ là $\min(b_i, c_i)$ trong (b, c); có số mũ là $\max(a_i, b_i)$ trong [a, b], là $\max(a_i, c_i)$ trong [a, c]; trong [a, (b, c)] số mũ của p_i là $\max(a_i, \min(b_i, c_i))$, còn trong ([a, b], [a, c]) số mũ của p_i là $\min[(\max(a_i, b_i), \max(a_i, c_i)]$.

Áp dụng đẳng thức A = B, suy ra điều phải chứng minh.

1.55 – $10^2 \equiv 0 \pmod 4$, $10^3 \equiv 0 \pmod 8$

1.56 – Đối với những bài toán loại này, hướng chung là tính toán để đi đến $a \equiv b \pmod m$, với b là số có trị tuyệt đối nhỏ nhất có thể được (tốt nhất là $b = \pm 1$), từ đó tính được thuận lợi $a^n \equiv b^n \pmod m$.

a/ $3.4 \equiv 2.6 \equiv 7.8 \equiv 1 \pmod{11}$. Số dư là 5.

b/ Theo mod 9: $1532 \equiv 2$, $1532^5 - 1 \equiv 2^5 - 1$

c/ Theo mod 83: $3^4 = 81 \equiv -2$, $3^{40} \equiv (-2)^{10} \equiv 28$

d/ Theo mod 25: $2^5 \equiv 7$, $2^{10} \equiv 7^2 \equiv -1$

$2^{1000} \equiv (-1)^{100} \equiv 1$

e/ Theo mod 13: $3012 \equiv 9$, $3012^3 \equiv 9^3 \equiv 1$

$3012^{93} \equiv 3012^{3.31} \equiv 1^{31} \equiv 1$

g/ Theo mod 11: $4362 \equiv 16$, $4362^2 \equiv 36 \equiv 3$

$4362^4 \equiv 9$, $4362^5 \equiv 9.6 \equiv -1$

$4362^{4362} \equiv 4362^{4360+2} \equiv (-1)^{872}.3 \equiv 3$

h/ Theo mod 425 : $35^2 = 1225 \equiv -50$, $35^3 \equiv -1750 \equiv -50$

$35^4 \equiv 2500 \equiv -50$, $35^{150} \equiv -50$

i/ $10^6 \equiv 1 \pmod 7$, $10^n \equiv 4 \pmod 6 \Rightarrow 10^n = 6k + 4$

$10^{10^n} = 10^{6k+4} \equiv 10^4 \pmod 7$

$A \equiv 10^4 + 10^4 + \ldots + 10^4 = 10.10^4 = 10^5 \equiv 5 \pmod 7$

1.57 a/ Chú ý rằng $2^{999} = 2^{1000} : 2$. Theo 1.56d thì 2^{1000} chia cho 25 dư là 1, do đó hai chữ số sau cùng của 2^{1000} có thể là 01, 26, 51 hoặc 76; nhưng 2^{1000} là bội của 4, nên 2^{1000} phải tận cùng bằng 76. Chia số này cho 2, thì hai chữ số sau cùng chỉ có thể 38 (=76 : 2) hoặc 88 (= 176 : 2). Nhưng 2^{999} là bội của 4, nên hai chữ số sau cùng của nó là 88 (bội của 4)

b/ Theo mod 100: $3^4 = 81 \equiv 19$, $3^8 \equiv 19^2 \equiv 61$

$3^{10} \equiv 61.9 \equiv 49$, $3^{20} \equiv 49^2 \equiv 01$

$3^{1000} \equiv 01 \pmod{100}$

nghĩa là hai chữ số sau cùng của 3^{1000} là 01. Số 3^{1000} là bội số của 3, nên chữ số hàng trăm của nó khi chia 3 phải cho số dư là 2 (chia tiếp thì 201 chia hết cho 3; nếu số dư là 0 hay 1 thì 001, 101 không chia hết cho 3). Vậy số $3^{999} = 3^{1000} : 3$ có hai chữ số sau cùng là 67 (= 201 : 3)

1.58 – a/ $2^4 = 16 \equiv 1 \pmod{15}$

b/ $2^4 \equiv 3 \pmod{13}$, $2^6 \equiv 12 \equiv -1 \pmod{13}$

$2^{70} = (2^6)^{11} . 2^4 \equiv -3 \pmod{13}$

$3^3 = 27 \equiv 1 \pmod{13}$', $3^{70} = (3^3)^{23} . 3 \equiv 3 \pmod{13}$

c/ Tìm số dư khi chia $20^{15} - 1$ cho 11, 31, 61.

Thí dụ theo mod 11:

$$20 \equiv -2 , 20^{15} \equiv (-2)^{15} , (-2)^5 = -32 \equiv 1$$

$$20^{15} \equiv (-2)^{15} \equiv (-2)^{5.3} \equiv 1$$

d/ Mod 7: $1890 \equiv 0$, $1945 \equiv -1$

e/ Mod 133: $12^2 = 144 \equiv 11$, $11^2 = 121 \equiv 12$

$$12^{2n+1} = 12.(12^2)^n \equiv 12.11^n , 11^{n+2} = 11^2 . 11^n \equiv 12.11^n$$

1.59 $2222 \equiv 3 \pmod 7$, $2222^4 \equiv 3^4 \equiv 4 \pmod 7$, $2222^5 \equiv 4.3 \equiv 5 \pmod 7$

$$5555 \equiv 4 \pmod 7 , 5555^2 \equiv 4^2 \equiv 2 \pmod 7$$

$$2222^{5555} + 5555^{2222} = 2222^{5.1111} + 5555^{2.1111}$$

$$\equiv 5^{1111} + 2^{1111} = (5 + 2).M \equiv 0 \pmod 7$$

1.60 – a/ $10a \equiv -b \pmod 7$, $3a \equiv -b \pmod 7$

$$27a^3 \equiv -b^3 \pmod 7 , -a^3 \equiv -b^3 \pmod 7$$

b/ $2^3 \equiv 1 \pmod 7$', $2^{3k} \equiv 1 \pmod 7$, $2^{3k+1} \equiv 2$, $2^{3k+2} \equiv 4 \pmod 7$

1.61 – a/ $x \equiv 3 \pmod{11}$; b/ $x \equiv 12 \pmod{13}$

c/ Cộng 2ab vào vế phải (điều có thể làm được):

$(a + b)x \equiv (a + b)^2 \pmod{ab} \Leftrightarrow x \equiv a + b \pmod{ab}$

(có thể chia hai vế của phương trình cho a + b, vì $(a, b) = 1$ nên $(a + b, ab) = 1$)

1.62 – a/ $2x \equiv 9 \pmod{11}$, $x \equiv 10 \pmod{11}$. Phương trình đã cho $6x \equiv 27 \pmod{33}$ có *ba nghiệm* là $x \equiv 10, 21, 32 \pmod{33}$

b/ $(a + 1, m) = 1 \Rightarrow$ nghiệm duy nhất $x \equiv a - 1 \pmod m$

$(a + 1, m) = d > 1 \Rightarrow$ d nghiệm:

$$x \equiv a - 1 , a - 1 + \frac{m}{d}, \dots a - 1 + \frac{(d-1)m}{d} \pmod m$$

1.63. Khi x chạy qua m giá trị khác nhau từ 0 đến m – 1 thì ax lấy m giá trị khác nhau:

$$ax_1 \equiv b_1 \pmod{m}$$

$$ax_2 \equiv b_2 \pmod{m}$$

....

$$ax_m \equiv b_m \pmod{m}$$

trong đó $x_1, x_2, ..., x_m$ đôi một khác nhau và lấy giá trị từ 0 đến m – 1, và $b_1, b_2, ... b_m$ cũng lấy giá trị từ 0 đến m – 1.

Phải chứng minh rằng $b_1, b_2, ..., b_m$ cũng đôi một khác nhau.

Thật vậy, giả sử có x_i và x_j $(x_i \neq x_j)$:

$$ax_i \equiv b_i \pmod{m}$$

$$ax_j \equiv b_j \pmod{m}$$

mà $b_i = b_j$ thì $a(x_i - x_j) \equiv 0 \pmod{m}$

Do $(a, m) = 1$ nên $x_i = x_j$, trái với giả thiết.

Nếu dùng kí hiệu tập hợp, ta có:

$\{x_1, x_2...x_m\} = \{b_1, b_2, ...b_m\} = \{0, 1,...m - 1\}$

1.64 Cho mỗi học sinh mang một số $n \equiv q \pmod{40}$, với q từ 0 (em cầm bóng ban đầu) đến 39, theo chiều từ phải sang trái của mỗi em.

Em cầm bóng ban đầu mang số 0 (7. 0)

Sau lần ném thứ 1, em nhận bóng mang số 7.1 (= 7)

Sau lần ném thứ 2, em nhận bóng mang số 7.2 (= 14)

....

Sau lần ném thứ 7, em nhận bóng mang số $7.7 = 49 \equiv 9 \pmod{40}$ (em này mang số 9)

....

Sau lần ném thư x , em nhận bóng mang số $7.x \equiv b \pmod{40}$

$$0 \leq b < 40$$

Khi x chạy qua các giá trị từ 0 đến 39 thì b cũng qua 40 giá trị đó (bài 1.63), nghĩa là mỗi học sinh đều nhận được bóng sau 40 lần ném (em cầm bóng ban đầu coi như nhận được bóng do một người "ngoài vòng" ném cho, đó là lần ném thứ 0)

1.65 a/ Vì pQr.b và pqR.c chia hết cho p nên

$$x_0 = Pqr.a + pQr.b + pqR.c \equiv Pqr.a \pmod{p}$$

Mà $Pqr \equiv 1 \pmod{p}$, nên $x_0 \equiv c \pmod{r}$

Tương tự : $x_0 \equiv b \pmod{q}$ và $x_0 \equiv c \pmod{r}$

b/ Đối với bài toán "Hàn Tín điểm binh", ta có

$p = 3, q = 5, r = 7$

$Pqr = P.5.7 \equiv 1 \pmod{3} \Rightarrow P = 2$ và $Pqr = 2.5.7 = 70$

$pQr = 3.Q.7 \equiv 1 \pmod{5} \Rightarrow Q = 1$ và $pQr = 3.7 = 21$

$pqR = 3.5.R \equiv 1 \pmod{7} \Rightarrow R = 1$ và $pqR = 3.5 = 15$

Nghiệm của hệ phương trình là

$x \equiv 70a + 21b + 15c \pmod{105}$

1.66

$$\begin{cases} x \equiv 1 \pmod{3} \\ x \equiv 3 \pmod{5} \\ x \equiv 4 \pmod{9} \\ x \equiv 9 \pmod{11} \\ x \equiv -167 \pmod{495}, \ x = 328, 823 \end{cases}$$

1.67 Giải hệ phương trình:

$$\begin{cases} x \equiv 1 \pmod{12} \\ x \equiv 1 \pmod{19} \\ x \equiv 14 \pmod{17} \end{cases}$$

Từ hai phương trình đầu, có $x \equiv 1 \pmod{12.19}$

$$x = 1 + 288t \ (12.19 = 228)$$

Thay vào phương trình cuối, có

$228t \equiv 13 \pmod{17}$

$t \equiv 14 + 17k$

Do đó $x = 1 + 228t = 1 + 228(14 + 17k)$

$x = 3193 + 3876k$

$k = 0$ thì $x = 3193$ (số hộc trong mỗi thùng). Giáp lấy 3192 hộc, Bính lấy 3192 hộc. Ất lấy 3179 hộc. Đó là đáp số trong "Số thư cửu chương" của Tần Cửu Thiều.

1.68 – a/ $x \equiv 49 \pmod{420}$ b/ vô nghiệm

1.69 – a/ $\begin{cases} x \equiv a \pmod 6 \\ x \equiv 1 \pmod 8 \end{cases} \Leftrightarrow \begin{cases} 4x \equiv 4a \pmod{24} \\ 3x \equiv 3 \pmod{24} \end{cases}$

$x \equiv 4a - 3 \pmod{24}$, với điều kiện của a:

$x = a + 6t = 1 + 8k \Rightarrow a = 1 + 2(3t + 4k) \Rightarrow a \equiv 1 \pmod 2$

b/ Từ hai phương trình sau, do $(21, 35) = 7$, ta có điều kiện của để hệ có nghiệm.

$a + 35t = 8 + 21k \Rightarrow a = 8 + 7(3k - 5t) \Leftrightarrow a \equiv 1 \pmod 7$

Chú ý rằng $[8, 21, 35] = 8.3.7.5 = 840$, từ hai phương trình đầu của hệ có:

$$\begin{cases} 21x \equiv 105 \pmod{21.8} \\ 8x \equiv 64 \pmod{21.8} \end{cases} \Leftrightarrow \begin{cases} 21x \equiv 105 \pmod{21.8} \\ 16x \equiv 128 \pmod{21.8} \end{cases}$$

$$\begin{cases} 5 \equiv -23 \pmod{21,8} \\ x \equiv a \pmod{7.5} \end{cases} \Leftrightarrow \begin{cases} 25x \equiv -115 \pmod{3.7.8.5} \\ 24x \equiv 24a \pmod{3.7.8.5} \end{cases}$$

Hệ có nghiệm là $x \equiv -115 - 24a \pmod{840}$

1.70 a/ $(18,20) = 2 \Rightarrow a + 18t = 11 + 20k \Leftrightarrow a \equiv 1 \pmod 2$

$(18,15) = 3 \Rightarrow a \equiv 1 \pmod 3$

Hệ có nghiệm khi và chỉ khi $a \equiv 1 \pmod 6$

b/ $3x \equiv 4 \pmod{10} \Leftrightarrow x \equiv 8 \pmod{10}$

$2x \equiv a \pmod 8$ có nghiệm khi và chỉ khi $a \equiv 0 \pmod 2$, tức $a = 2k$.

Ta có hệ $x \equiv 8 \pmod{10}$

$x \equiv k \pmod 4$

(10,4) = 2, nên hệ này có nghiệm khi và chỉ khi $k - 8 \equiv 0 \pmod 2$ tức $k \equiv 0 \pmod 2$. Hệ đã cho có nghiệm khi và chỉ khi $a \equiv 0 \pmod 4$

1.71 $10^2 \equiv 1 \pmod 3 \Rightarrow 99 \vdots 3$; $10^6 \equiv 1 \pmod 7 \Rightarrow 999999 \vdots 7$

$10^{10} \equiv 1 \pmod{11}$, $10^{12} \equiv 1 \pmod{13}$ và $10^{16} \equiv 1 \pmod{17}$

Chú ý rằng có trường hợp ta không có số *nhỏ nhất* có tính chất đó, thí dụ $10 - 1 = 9 \vdots 3$, $10^2 - 1 = 99 \vdots 11$

1.72 $a^4 \equiv 1 \pmod 5$, với $a = 1, 2, 3, 4 \Leftrightarrow a^{4k} \equiv 1 \pmod 5$

1.73 $a^2 \equiv a \pmod 2 \Rightarrow a^4 \equiv a^2 \equiv a \pmod 2 \Rightarrow a^5 \equiv a \pmod 2$

$a^3 \equiv a \pmod 3 \Rightarrow a^5 \equiv a^3 \equiv a \pmod 2$

$a^5 \equiv a \pmod 5$. Vậy $a^5 \equiv a \pmod{2.3.5}$

Do đó $a_1^5 + a_2^5 + \dots + a_n^5 \equiv a_1 + a_2 + \dots + a_n \pmod{30}$

1.74 $240 = 2^4.3.5$, $(a, 240) = 1 \Rightarrow (a, 2) = (a, 3) = (a, 5) = 1$

$(a, 6) = 1 \Rightarrow a^2 \equiv 1 \pmod{24}$, xem bài tập 1.13

$(a, 2) = 1 \Rightarrow a^2 \equiv -1 \pmod 2$

Mà $a^4 - 1 = (a^2 - 1)(a^2 + 1)$, nên $a^4 \equiv 1 \pmod{48}$

$(a, 5) = 1 \Rightarrow a^4 \equiv 1 \pmod 5$. Vậy $a^4 \equiv 1 \pmod{48.5}$

1.75 $42p = 2.3.7.p$. Ta chứng minh $A = 3^p - 2^p - 1 \vdots 2.3.7.p$

a/ $3^p - 1 \equiv 0 \pmod 2 \Rightarrow A \equiv 0 \pmod 2$

b/ $2^p + 1 \equiv 0 \pmod 3 \Rightarrow A \equiv 0 \pmod 3$

c/ $3^p \equiv 3 \pmod p$ và $2^p \equiv 2 \pmod p$ $A \equiv 3 - 2 - 1 = 0 \pmod p$

d/ p nguyên tố, chỉ có thể có dạng $6t + 1$ hoặc $6t + 5$

$p = 6t + 1 \Rightarrow A = 3^{6t+1} - 2^{6t+1} - 1 = 3(3^{6t} - 1) - 2(2^{6t} - 1) \equiv 0 \pmod 7$

vì $3^6 \equiv 1 \pmod 7$ và $2^6 \equiv 1 \pmod 7$

$p = 6t + 5 \Rightarrow A = 3^5(3^{6t} - 1) - 2^5(2^{6t} - 1) + 3^5 - 2^5 - 1 \equiv 0 \pmod 7$

1.76 a/ $n = 1$

b/ Theo định lý Fermat: $2^p \equiv 2 \pmod p$, theo giả thiết

$\Rightarrow 2^p \equiv -1 \pmod p$

$\Rightarrow 3 \equiv 0 \pmod p \Rightarrow p = 3$. Với $p = 3$ thì $2^p + 1 = 9$

$\equiv 0 \pmod 3$

1.77 $1 \le \varphi(n) < n \Rightarrow n! \equiv 0 \pmod{\varphi(n)}$

$(2, n) = 1 \Rightarrow 2^{\varphi(n)} \equiv 1 \pmod n \Rightarrow 2^{n!} \equiv 1 \pmod n$

1.78 $m^{\varphi(n)} \equiv 1 \pmod n$, $n^{\varphi(m)} \equiv 1 \pmod m$

$\Rightarrow m^{\varphi(n)} + n^{\varphi(m)} \equiv 1 \pmod n$ và $n^{\varphi(m)} + m^{\varphi(n)} \equiv 1 (mod m)$

$(m, n) = 1 \Rightarrow m^{\varphi(n)} + n^{\varphi(m)} \equiv 1 \pmod{mn}$

1.79 $p = 2$ thì mọi số $2^n - n$, với $n = 2k$ ($k \in N$), chia hết cho p.

$p > 2 \Rightarrow 2^{p-1} \equiv 1 \pmod p \Rightarrow 2^{m(p-1)} \equiv 1 \pmod p$, $m \in N$

Lấy $m \equiv -1 \pmod p$, tức $m = kp - 1$;

$2^{m(p-1)} - m(p - 1) = 2^{m(p-1)} + m - mp \equiv 1 - 1 = 0 \pmod p$

Vậy mọi số $2^n - n$ với $n = (kp - 1)(p - 1)$, $k \in N$, chia hết cho p.

1.80 $a^{10} \equiv 1 \pmod{11} \Rightarrow a^{30} \equiv 1 \pmod{11}$, với $a = 1, 2, \dots 10$

2.1 – Số nguyên tố p : a/ đều là số lẻ b/ $(p, 2) = (p, 3) = 1$

2.2 – $(p - 1)(p + 1) \vdots 8$ (do p lẻ)

$p = 6n \pm 1 \Rightarrow p^2 - 1 \vdots 3$. Vậy $p^2 - 1 \vdots 24$

$p^2 - q^2 = (p^2 - 1) - (q^2 - 1) \vdots 24$

2.3 $p = 2$ thì $8p + 1$ là nguyên tố, $8p - 1$ là hợp số

$p = 3$ thì $8p + 1$ là hợp số, $8p - 1$ là nguyên tố.

$p \ne 3 \Rightarrow 8p - 1$, $8p$ và $8p + 1$ là ba số liên tiếp, trong đó phải có một số là bội của 3; p nguyên tố nên 8p không chi hết cho 3, do đó nếu một trong hai số $8p - 1$ và $8p + 1$ là nguyên tố thì số kia là hợp số (bội của 3)

2.4 – a/ $4p$, $4p + 1$, $4p + 2 = 2(2p + 1)$ là ba số liên tiếp; do p và $2p + 1$ là nguyên tố ($p > 3$), nên $4p$ và $4p + 2$ không chia hết cho 3. Do đó $4p + 1$ là hợp số (bội của 3)

b/ $p > 3 \Rightarrow 8p^2 + 1 \equiv 3$.

Với $p = 2, 3$ thì $8p^2 - 1$ và $8p^2 + 2p + 1$ đều là nguyên tố (31, 71; 37, 79)

2.5 – a/ $2p + 1 = n^3 \Rightarrow 2p = n^3 - 1 = (n - 1)(n^2 + n + 1)$

$p \neq 2$ (thử) $\Rightarrow (2, p) = 1 \Rightarrow n - 1 = 2$

và $n^2 + n + 1 = p$

(không có $n^2 + n + 1 = 2$) $\Rightarrow p = 13$

(thử lại: $2.13 + 1 = 27 = 3^3$)

b/ $13p = n^3 - 1 = (n - 1)(n^2 + n + 1)$

$(13, p) = 1 \Rightarrow n - 1 = 13$ $(n = 14)$ hoặc

$n^2 + n + 1 = 13$ $(n = 3)$

$\Rightarrow$ $p = 211$ và $p = 2$

2.6 Trong ba số liên tiếp $2^n - 1$, 2^n, $2^n + 1$ có một số chia hết cho 3.

Số 2^n chỉ chứa thừa số 2 nên không thể là bội của 3. Do đó $2^n - 1$ và $2^n + 1$ không thể đồng thời là nguyên tố (có một là bội của 3). Chúng có thể là hợp số cả, thí dụ với $n = 6$, có $2^6 - 1 = 63 \,\vdots\, 3$ và $2^6 + 1 = 65 \,\vdots\, 5$.

2.7 – a/ $p = 3 \Rightarrow p + 10 = 13$ và $p + 14 = 17$ đều là nguyên tố.

$p \neq 3 \Rightarrow p = 3k \pm 1 \Rightarrow p + 10$ hoặc $p + 14$ là hợp số.

b/ $p = 5$.

c/ $p = 5$. Nếu $p \neq 5$, tức $p = 5k \pm 1$, $5k \pm 2$ thì một trong bốn số

$p + 6 = p + 1 + 5$, $p + 8 = p + 5 + 3$,

$p + 12 = p + 10 + 2$, $p + 14 = p + 10 + 4$ là bội của 5.

2.8 $p = 30q + r = 2.3.5q + r$, $r < 30$ mà không thể có ước nguyên tố là 2, 3, 5 vậy $r = 1$ hoặc r nguyên tố $(5 < \sqrt{29} < 7)$.

$p = 60q + r = 2.2.3.5.q + r$, $0 < r \leq 59$,

mà $7 < \sqrt{59} < 11$, r có thể là $7^2 = 49$.

2.9 – Trong 10 số liên tiếp, có 5 số chẵn (trong đó nhiều nhất là một số nguyên tố là 2) và 5 số lẻ. Vậy có không quá 6 số nguyên tố.

$k = 0$; từ 1 đến 10 có 4 số nguyên tố (2, 3, 5, 7)

$k = 1$; từ 2 đến 11 có 5 số nguyên tố (2, 3, 5, 7, 11)

$k > 1$; từ 3 trở đi, không có số chẵn nào là nguyên tố; trong 5 số lẻ liên tiếp, có một số là bội của 3; do đó trong dãy có ít hơn 5 số nguyên tố.

Tóm lại: $k = 1$ (có 5 số nguyên tố)

2.10 p, $p + 2$ và $p + 4$ (p lẻ)

$p = 3 \Rightarrow 3, 5, 7$ là nguyên tố.

$p > 3 \Rightarrow p = 3k + 1 \Rightarrow p + 2 \vdots 3$

$p = 3k + 2 \Rightarrow p + 4 \vdots 3$

Chỉ có bộ ba duy nhất 3, 5, 7.

2.11 $p^2 + q^2 + r^2$ là số nguyên tố lẻ (> 2) $\Rightarrow p^2, q^2, r^2$ đều lẻ $\Rightarrow p, q, r$ đều lẻ.

Nếu cả ba số nguyên tố p, q, r đều khác 3 (không chia hết cho 3) thì $p^2 + q^2 + r^2$ là bội của 3 (hợp số).

Nếu $p = 3$ thì $q = 5$, $r = 7$. Bộ ba số nguyên tố liên tiếp duy nhất: 3, 5, 7 mà $3^2 + 5^2 + 7^2 = 83$ là nguyên tố.

2.12 – p phải lẻ: $p = p_1 + p_2 = p_3 - p_4 \Rightarrow p_1$ hoặc p_2 chẵn ($= 2$) và p_4 chẵn $\Rightarrow p = p_1 + 2 = p_3 - 2$ ($\Rightarrow p_3 = p_1 + 4$)

$\Rightarrow p_1, p_1 + 2, p_1 + 4$ đều là nguyên tố. Chỉ có $p_1 = 3$ (bài 2.10)

$\Rightarrow p = 5$ ($5 = 3 + 2 = 7 - 2$)

2.13 – a/ $n^4 + 4 = (n^2 + 2)^2 - 4n^2 = (n^2 + 2 - 2n)(n^2 + 2 + 2n)$ là số nguyên tố với giá trị duy nhất $n = 1$ ($n^4 + 4 = 5$)

b/ $n^4 + n^2 + 1 = (n^2 + 1)^2 - n^2 = (n^2 + 1 - n)(n^2 + 1 + n)$, tương tự a/

c/ $n^3 - n^2 + n - 1 = (n - 1)(n^2 + 1)$

là số nguyên tố chỉ với $n = 2$.

2.14 – a/ $\dfrac{n(n + 1)}{2} - 1 = \dfrac{(n - 1)(n + 2)}{2} = N$

$n = 2$ và $n = 3$ thì N là nguyên tố (2 và 5)

$n > 3 \Rightarrow N$ là hợp số.

b/ $\frac{n(n+1)(n+2)}{6} + 1 = \frac{(n+3)(n^2+2)}{6} = N$

$n = 1, 2, 3$ có các số nguyên tố (2, 5, 11); $n \geq 4 \Rightarrow N$ hợp số.

2.15 – Lấy $n = 4k^4 \Rightarrow m^4 + n = m^4 + 4k^4 = (m^2 + 2k^2)^2 - (2mk)^2$

$$= (m^2 + 2k^2 - 2mk)(m^2 + 2k^2 + 2mk)$$

2.16 – $(n - 1)! = 1.2...(n - 1) \vdots n$, nếu n là nguyên tố thì nó phải là ước nguyên tố của một số từ 1 đến $n - 1$. Ước nguyên tố của một số không thể lớn hơn số đó.

2.17 – a/ N chẵn, nhưng không là bội của 4.

$N = 1 = k^2$ (N + 1 lẻ, k lẻ) $\Rightarrow N = (k - 1)(k + 1) : 4$, vô lý.

b/ $N \vdots 3$. Nếu $N - 1 = k^2 \Rightarrow N - 1 = 3q - 1 = k^2$; thì vô lý (bình phương của mọi số k đều có dạng 3q hay 3q + 1)

2.18 – a/ $x^3 + 1 = (x + 1)(x^2 - x + 1)$. Với $x = 1$, có số nguyên tố 2, $x > 1$ thì $x^3 + 1$ là hợp số.

b/ $x = 1, 3, 5$.

2.19 – Tương tự với chứng minh: có vô số nguyên tố dạng $3x - 1$ ($x \geq 1$), xem tr 56.

Tích của hai số dạng $4x + 1$ cũng là số có dạng $4x + 1$, nên trong các ước số có dạng $4x + 3$ phải có ít nhất một số dạng $4x + 3$. Lập số $4(2.3....p) - 1 = M$ (có dạng $4x - 1$, cũng là dạng $4x + 3$)

Số có dạng $6x + 5$ (hay $6x - 1$) phải có ít nhất một ước số dạng $6x + 5$. Lập số $6(2.3...p) - 1 = M$.

2.20 – $2n + 1 > 7 \Rightarrow 2n + 1 - 3 = 2(n - 1) > 4$. Theo giả thuyết Goldbach-Euler, số chẵn $2(n - 1) > 4$ là tổng của hai số nguyên tố $p + q$, và cả p, q đều lẻ. Như vậy, $2n + 1 = 3 + p + q$, tổng của ba số nguyên số lẻ.

3.1 – a/ $x = -2 + 3t$, $y = 4 - 5t$

b/ $16x - 20y = 19$, $(16, 20) = 4$, phương trình không có nghiệm nguyên.

c/ Giải $38x + 117y = 1$

$117 = 38.3 + 3,\ 38 = 3.12 + 2,\ 3 = 2.1 + 1,\ 3 + \dfrac{1}{12+1} = \dfrac{40}{13}$

$\Rightarrow x_0 = -40,\ y_0 = 13 \Rightarrow$ phương trình đã cho có nghiệm tổng quát

là $\begin{cases} x = -40.15 + 117t \\ y = 13.16 - 38t \end{cases}$ $(t \in Z)$

d/ $x_0 = 4.3 = 12$, $y_0 = 5.3 = 15$.

3.2 $7x = 60y + 1$, trong đó 60 là BCNN của 2, 3, 4, 5, 6.

$x = -17 + 60t$, số phải tìm là $7x = -119 + 420t$.

3.4. Ta biết Nguyễn Du sống không đến 86 tuổi. Vì vậy năm sinh là $\overline{17xy}$ và ta có phương trình:

$1786 - \overline{17xy} = 1 + 7 + x + y\ (0 \le x \le 8, 0 \le y \le 9)$

$1786 - (1700 + 10x + y) = 8 + x + y$

$11x + 2y = 78$

Nghiệm thích hợp là $x_0 = y_0 = 6$. Đáp số 1766.

3.5 - Gọi x là số cá câu được và y là số cá còn lại sau khi cả ba người đã lấy đi phần cá của mình. Có phương trình

$$\frac{2}{3}\left\{\frac{2}{3}\left[\frac{2}{3}(x-1) - 1\right] - 1\right\} = y$$

$8x - 27y = 38 \qquad (x, y \in N)$

Áp dụng thuật toán Euclide, ta có một nghiêm riêng là

$x_0 = -10.38 = -380$, $y_0 = -3.38 = -114$, do đó:

$\begin{cases} x = -380 + 27t \\ y = -144 + 8t \end{cases}$

Giá trị dương nhỏ nhất của x , y (vì câu cá tồi!) ứng với $t = 15$, lúc đó $x = 25$, $y = 6$.

Chú ý. Áp dụng dụng thuật toán Euclide để tìm một nghiệm riêng của phương trình $ax + by = c$, ta có thể có các giá trị lớn (nhất là khi c lớn, như trong bài toán trên). Để có biểu thức đơn giản hơn của nghiệm tổng quát, ta chọn một giá trị riêng thích hợp của t (để c· nghiệm riêng có giá trị tuyệt đối bé)

Đối với phương trình $8x - 27y = 38$, trong biểu thức của nghiệm trên đây, cho $t = 14$ có $x_0 = y_0 = -2$; cho $t = 15$ có $x_0 = 25$, $y_0 = 6$ và nghiệm có thể viết dưới dạng

$$\begin{cases} x = -2 + 27t \\ y = -2 + 8t \end{cases} \text{ hay } \begin{cases} x = 25 + 27t \\ y = 6 + 8t \end{cases}$$

3.6 – a/ $x_0 = 2m + 4$; $y_0 = -m - 2$

b/ Điều kiện: $m - 1$ chia hết cho $(15, 25) = 5$, tức $m - 1 = 5k$

Lúc đó: $3x + 5y = k \Rightarrow x = 2k + 5t$

$y = -k - 3t$

c/ Điều kiện: $d = (3, m - 2) = 1$ hoặc 3; khi $d = 3$ thì $m + 1 \vdots 3$

$$x_0 = 1,\ y_0 = -1,\quad x = 1 + m - \frac{m-2}{d}t$$

$$y = -1 + \frac{3}{d}t$$

d/ Điều kiện: $d = (5, 3m + 1) = 1$ hoặc 5

$d = 5 \Rightarrow 3m + 1 = 5k \Rightarrow m = 5k + 3$

$\Rightarrow 2m + 1 = 5t + 2 \vdots 5$

$\Rightarrow$ Phương trình vô nghiệm.

Vậy phương trình có nghiệm nguyên khi và chỉ khi

$m \neq 5k + 3$ $(d = 1)$

$m = 5k \Rightarrow 5x + (15k + 1)y = 10k + 1$

$$x_0 = -k,\ y_0 = 1 \text{ và } \begin{cases} x = -k + (15k + 1)t \\ y = 1 - 5t \end{cases}$$

Xét tiếp $m = 5k + 1$, $5k + 2$, $5k + 4$.

3.7 $ax = b(a - y)$, $(a, b) = 1 \Rightarrow x \vdots b \Rightarrow x \geq b$

$ax \geq ab$. Mà $ax + by \geq ax$ nên $ax = by \geq ab$, trái với giả thiết.

3.8 – Lấy $a > m + n$, $b > m + n$ và $(a, b) = 1$, lấy $c = am + bn$.

$\Rightarrow ax + by = c$ có nghiệm nguyên dương $x = m$, $y = n$.

Đây là nghiệm nguyên dương duy nhất. Thực vậy, giả sử $x_1 \neq m, y_1 \neq n$

$(x_1, y_1 > 0)$ mà $ax_1 + by_1 = c$ $(= am + bn)$

Không thể là $x_1 \geq m, y_1 > n$ hoặc $x_1 > m, y_1 \geq n$, vì như thế thì $ax_1 + by_1 > am + bn = c$

Vậy $y_1 < m$ hoặc $y_1 < n$

$$x_1 < m \Rightarrow 0 < m - x_1 < m \Rightarrow by_1 = a(m - x_1) + bn$$

$$\Rightarrow a(m - x_1) \vdots b \Rightarrow m - x_1 : b \text{ do } (a, b) = 1$$

Điều này vô lý vì $b > m + n > m$

Tương tự với $y_1 < n$.

13.9 Lấy phương trình $x + y = m + 1$, có đúng m nghiệm nguyên dương.

$$x = t, y = m - t + 1 \ (t = 1, 2, ..., m)$$

3.10 - a/ $x = 6 - u - 3t$, $y = 1 - u + 2t$, $z = u$ $(u, t \in Z)$

b/ $x = 9 - 15u + 53t$, $y = 2 - 5u + 23t$, $z = u$ $(u, t \in Z)$

c/ Hệ số của x và của z bằng nhau.

d/ $(8, 15) = 1$

3.11 - a/ $x = 1 + 12t$, $y = -1 - 3t$, $z = 1 + 6t$ $(t \in Z)$

b/ $x = -1 - 9t$, $y = -1 - 6t$, $z = 2 + 5t$ $(t \in Z)$

3.12 - a/ $3x + 2y = 1 \Leftrightarrow x = 1 + 2t$, $y = -1 - 3t$ $(t \in Z)$

Thay vào phương trình thứ hai, có:

$$(m + 1)z - 12t = m + 1 \Leftrightarrow t = \frac{m+1}{d}k, \ z = 1 + \frac{12}{d}k \ (k \in Z)$$

trong đó $d = (m + 1, 12)$. Suy ra x, y.

b/ $3x - 5y = 1 + 3z \Leftrightarrow x = 2 + 6z + 5t$

$y = 1 + 3z + 3t$ $(z, t \in Z)$

Thay vào phương trình thứ hai, được

$$t - (m + 1)z = m \quad \Leftrightarrow \quad \begin{cases} z = -1 + u \\ t = -1 + (m+1)u \end{cases}$$

Kết quả $x = 5mu + 11u - 9$

$y = 3mu + 6u - 5$

$z = -1 + u \ (u \in Z)$

3.13 – a/ $x = 9u$, $x + 1 = 25v$ $(u, v \in N) \Rightarrow 25v - 9u = 1$,

$v = 4 + 9t$, $u = 11 + 25t \Rightarrow x = 99 + 225t \ (t \in N)$

b/ $x = 21u$, $x + 1 = 165v \Rightarrow 165v - 21u = 1$,

$(165, 21) \neq 1 \Rightarrow$ phương trình không có nghiệm nguyên.

c/ Theo a/: $x = 99 + 225t$

Lại có $x + 2 = 4y$

$\Rightarrow 101 + 255t = 4y \Rightarrow t = -101 + 4k$, $k \geq 26$ để $t > 0$

$x = -22626 + 900k$, $k \geq 26$

3.14 $x = 23 + 209t$

3.15 $x = -2 + 35t$

3.16 $\begin{cases} 3x - y + 1 = 7u \\ 2x + 3y - 1 = 7v \end{cases} \Leftrightarrow \begin{cases} 9x - 3y + 3 = 21u \\ 2x + 3y - 1 = 7v \end{cases}$

$\Rightarrow 11x + 2 = 7(3u + v) \Rightarrow x = 3 + 7t$

$y = 3 + 7k \ (t, k \in Z)$

3.17 $x = 4u + 3 = 5v + 4 = 7t + 5 \Rightarrow x = 19 + 140k$

$x = 299, 439$

3.18 $x = 262$

3.19 $x + y + z = 100$

$$3 + \frac{y}{5} + 5z = 60$$

$\Rightarrow 7x + 12z = 100 \Rightarrow x = 4, z = 6, y = 90$

3.20 – a/ $8x - 13y + 6 = 0$ với $-10 < x < 50$

b/ $3x + 5y = 7$ với $6 < x < 42$ và $2 < y < 17$

3.21 x, y phải cùng chẵn hoặc cùng lẻ $\Rightarrow x + y$ và $x - y$ cùng chẵn.

$x + y = 2u$, $x - y = 2v \Rightarrow 4u^2 + 4v^2 = (x + y)^2 + (x - y)^2 = 2(x^2 + y^2) = 4z^2 \Rightarrow u^2 + v^2 = z^2$.

Giải phương trình này, lấy $x = u + v$, $y = u - v$.

3.22 - Bộ ba số $x = 2m^2 - 1$, $y = 2m$, $z = 2m^2 + 1$ ($m \in N$) là nghiệm của phương trình.

Ghi chú. Có thể áp dụng phương pháp giải $x^2 + y^2 = z^2$ để giải

$$ax^2 + y^2 = z^2.$$

3.23 Dùng hằng đẳng thức $(n^2 + n - 1)^2 + (2n + 1)^2 = (n^2 + n + 1)^2 + 1$.

Với $n = 1, 2, 3$ có $5^2 + 5^2 = 7^2 + 1$, $11^2 + 7^2 = 13^2 + 1$

$$19^2 + 9^2 = 21^2 + 1$$

cũng có: $[2n(4n + 1)]^2 + (16n^3 - 1)^2 = (16n^3 + 2n)^2 + 1$

từ đó, có chẳng hạn: $10^2 + 15^2 = 18^2 + 1$, $36^2 + 127^2 = 132^2 + 1$

3.24 $(x + 2y)(x - 2y) = 1 \Rightarrow 1 : (x + 2y) \Rightarrow x = \pm 1, y = 0$

3.25 $(x + y)(x - y) = 91$. Xét mọi trường hợp xảy ra với

$91 = (\pm 1)(\pm 91) = (\pm 13)(\pm 7)$. Có 8 nghiệm nguyên.

3.26 x , y, z có ước chung $d > 1$: $x = dx'$, $y = dy'$, $z = dz'$

$\Rightarrow 2(dx')^2 + 3(dy')^2 = (dz')^2 \quad \Leftrightarrow \quad 2x'^2 + 3y'^2 = z'^2$

Vì vậy, có thể giả thiết $(x ,y, z) = 1$. Nói riêng x và z không là bội của 3 (nếu $x = 3u$, $z = 3v$ thì sẽ có $y = 3t$)

$\Rightarrow 2x^2 = z^2 - 3y^2$, tức $2x^2$ và z^2 có cùng số dư ($\neq 0$) khi chia cho 3, điều không thể có. Vậy phương trình vô nghiệm (không có nghiệm nguyên)

3.27 $x^2 + x - y^2 = 0 \Leftrightarrow x(x + 1) = y^2$ mà $(x,x + 1) = 1$. Phương trình vô nghiệm.

3.28 $(x - y)(x^2 + xy + y^2) = 7(x - y) \Leftrightarrow x^2 + xy + y^2 = 7$ (với $x \neq y$)

$$(x - y)^2 = 7 - 3xy \Rightarrow 7 - 3xy > 0,\ xy < 7/3$$

Hai nghiệm ($x = 1$; $y = 2$), ($x = 2$; $y = 1$), *ngoài* $x = y$

3.29 $(x + 2y)(3x + 4y) = 96$. Chú ý rằng $(x + 2y) + (3x + 4y) = 4x + 6y = 2(2x + 3y)$. Hai số $x + 2y$ và $3x + 4y$ đều chẵn.

3.30 $(18x^2 + 27y^2) + (x^2 + y^2) = 3.243 \Rightarrow x^2 + y^2 \vdots 3$

$\Rightarrow x \vdots 3$ và $y \vdots 3$

$x = 3u,\ y = 3v \Rightarrow 19u^2 + 28v^2 = 81.$

tương tự: $u = 3s,\ v = 3r \Rightarrow 19s^2 + 28r^2 = 9.$

$\Rightarrow s = 3p,\ r = 3q \Rightarrow 19p^2 + 28q^2 = 1$

Vô nghiệm.

3.31 $-(x - 5)(y + 3) = -18$. Có 12 nghiệm nguyên.

3.32 $-(x - 1)(y - 1) = 1 \Leftrightarrow (x = 2, y = 2)$ và $(x = 0, y = 0)$

3.33 Có thể giả thiết $x \le y$

$x = y \Rightarrow 2x + 1 = x^2z \Leftrightarrow x(xz - 2) = 1 \Rightarrow x = 1, y = 1, z = 3$

$x < y \Rightarrow xyz < 2y + 1 \Leftrightarrow xyz \le 2y \Leftrightarrow xz \le 2 \Rightarrow x = 1$ hoặc 2

$x = 1 \Rightarrow y + 2 = yz\ (> 1) \Leftrightarrow y(z - 1) = 2 \Rightarrow y = 2,\ z = 2$

$x = 2 \Rightarrow y + 3 = 2yz \Leftrightarrow y(2z - 1) = 3$

$\Rightarrow y = 3$ (do $y > x$) và $z = 1$

Có ba nghiệm $(x \le y)$: $(1; 1; 3)$, $(1; 2; 2)$ và $(2; 3; 1)$

3.34 $x^3 = 2(y^3 + 2z^3) \Rightarrow x^3$ chẵn $\Rightarrow x$ chẵn : $x = 2x'$

$8x'^3 = 2(y^3 + 2z^3) \Rightarrow y^3 = 4x'^3 - 2z^3 \Rightarrow y = 2y'.$

Do đó $z = 2z'$.

$(2x')^3 = 2[(2y')^3 + 2(2z')^3] \Leftrightarrow x'^3 = 2(y'^3 + 2z'^3)$

Như vậy, nếu $(x ; y ; z)$ là nghiệm thì $\left(\frac{x}{2}; \frac{y}{2}; \frac{z}{2}\right)$ cũng là nghiệm. quá trình này tiếp diễn mãi được; $(x; y; z)$ chỉ có thể là $(0; 0; 0)$

3.35 $y^2 = x^3 + 7 \Rightarrow x$ phải lẻ, vì $(2k)^3 + 7 = 8k + 7$ không thể là số chính phương.

$y^2 + 1 = x^3 + 8 = (x + 2)(x^2 - 2x + 4)$

$x^2 - 2x + 4 = (x - 1)^2 + 3$ có dạng $4k + 3$ (x lẻ)

Mà số có dạng $4k + 3$ phải có một ước nguyên tố q có dạng đó (phân tích $4k + 3$ ra thừa số nguyên tố không thể chỉ gồm có các thừa số dạng $4k + 1$, vì tích của chúng là số có

dạng $(4k + 1)$; $y^2 + 1$ không thể là bội của q.

Phương trình vô nghiệm.

3.36 Tương tự bài 3.34.

(1) $x^2 + y^2 + z^2 = x^2y^2 \Rightarrow x$, y không thể đều là số lẻ.

(theo mod 4, nếu $x^2 \equiv y^2 \equiv 1$ thì $x^2y^2 \equiv 1 \Rightarrow x^2 + y^2 = z^2 \neq 1$)

x chẵn hoặc y chẵn $\Rightarrow x^2y^2 \vdots 4 \Rightarrow x^2 + y^2 + z^2 \vdots 4 \Rightarrow$

$\Rightarrow x = 2x_1, y = 2y_1, z = 2z_1 \Rightarrow x_1^2 + y_1^2 + z_1^2 = 4x_1^2y_1^2$ *(2)*

Như vậy, nếu x , y, z là nghiệm của phương trình (1) đã cho thì $x_1 = x / 2$, $y_1 = y/2$, $z_1 = z/2$ là nghiệm của (2).

Tiếp tục như vậy, có

$$x^2 = \frac{x_1}{2} (= x/4) , y_2 = \frac{y_1}{2} (= y/4), z_2 = \frac{z_1}{2} (= z/4)$$

là nghiệm của $x_2^2 + y_2^2 + z_2^2 = 16x_2^2 z_2^2$

Quá trình này có thể tiếp tục mãi, các số $\frac{x}{2^k}, \frac{y}{2^k}, \frac{z}{2^k}$ là số chẵn với mọi k. Do đó $(x; y; z)$ chỉ có thể là $(0; 0; 0)$

3.37 – Tương tự 3.36

3.38 – Tương tự 3.36.

3.39 Đặt $\frac{x}{u} = p , \frac{y}{u} = q , \frac{z}{u} = s$

$p^2 + q^2 + s^2 = 1 \Rightarrow p = 1$, $q = s = 0$ là một nghiệm.

Lại đặt $p = x_1 + 1$, $q = y_1$, $s = z_1$

$x_1 + y_1 + z_1 + 2x_1 = 0$. Giả sử $\frac{x_1}{z_1} = \frac{m}{n}, \frac{y_1}{z_1} = \frac{r}{n}$

$$\begin{cases} x = (r^2 + n^2 - m^2)t \\ y = 2mrt \\ z = 2mnt \\ u = (r^2 + n^2 + m^2)t \qquad t \in Z \end{cases}$$

3.40 $x = (p^2 + q^2 + r^2 - s^2)k$, $y = 2qsk$, $z = 2rsk$,

$u = 2psk$, $\qquad t = (p^2 + q^2 + r^2 + s^2)k$, $k \in Z$

3.41 Tương tự 3.36.

3.42 $y^2 = x(x + 8)(x + 1)(x + 7)$

$= (x^2 + 8x)(x^2 + 8x + 7) = z^2 + 7z$

$(z = x^2 + 8x)$. Nếu $z > 9$ thì

$(z + 3)^2 = z^2 + 6z + 9 < z^2 + 7z = y^2 < z^2 + 8z + 16$

$= (z + 4)^2$

y^2 nằm giữa bình phương của hai số liên tiếp, vô lý.

$\Rightarrow x^2 + 8x = z \le 9 \Rightarrow -9 \le x \le 1$. Thử các giá trị này của x, có $x = -9, -8, -7, -4, -1, 0, 1$ nghiệm đúng, từ đó có y tương ứng.

3.43 Tương tự 3.35

3.44 $x = 0$, $y = \pm 1$ là hai nghiệm duy nhất:

$x > 0 \Rightarrow (x^3 + 1)^2 < x^6 + 3x^3 + 1 = y^4 < x^6 + 4x^3 + 4$

$= (x^3 + 2)^2$

$\Rightarrow$ không có y^4, vì không có $x^3 + 1 < y^2 < x^3 + 2$

$x \le -2 \Rightarrow (x^3 + 2)^2 < x^6 + 3x^3 + 1 = y^4 < x^6 + 2x^3 + 1$

$= (x^3 + 1)^2$

$x = -1 \Rightarrow -1 = y^4$

3.45 Tương tự **3.44**

$y^3 = 8(x^3 + 3x^2 + 4x + 2) = (2z)^3$

với $z^3 = x^3 + 3x^2. + 4x + 2$.

$x \le 0 \Rightarrow (x + 1)^3 < z^3 < (x + 2)^3 \Rightarrow x + 1 < z < x + 2$, vô lý

$x \ge -2 \Rightarrow$ đặt $x_1 = -x - 2 \ge 0$, $y_1 = -y \Rightarrow x_1$ và y_1 thỏa mãn

$(x_1 + 2)^4 - x_1^4 = x^4 - (x + 2)^4 = -y^3 = y_1^3$

điều này không thể có với $x_1 \geq 0$.

$-2 < x < 0 \Rightarrow x = -1, y = 0$ là nghiệm duy nhất.

3.46 $n = 2k \quad \Rightarrow n^4 = 16k^4 \vdots 16$

$n = 2k + 1 \Rightarrow n^4 - 1 = (n - 1)(n + 1)(n^2 + 1) \vdots 16$

($n - 1$, $n + 1$, $n^2 + 1$ đều chẵn và một trong số $n - 1$, $n + 1$ chia hết cho 4). Như vậy, khi chia tổng $x_1^4 + x_2^4 + ... + x_{14}^4$ cho 16, có số dư bằng số các số lẻ trong $x_1, x_2 ..., x_{14}$, tức là không vượt quá 14. Còn 1599 = 1600 − 1, chia cho 16 có dư là −1, tức 15. Phương trình vô nghiệm.

3.47 – Phương trình $x^2 - y^2 = k$ có nghiệm nguyên $\Leftrightarrow k \neq 4t + 2$ $(t \in Z)$

a) $x^2 - y^2 = k$ có nghiệm nguyên $\Rightarrow k \neq 4t + 2$. Chỉ cần xét mọi trường hợp : x , y cùng chẵn, cùng lẻ, và một chẵn một lẻ.

b) $k \neq 4t + 2$: k chẵn $\Rightarrow k = 4m \Rightarrow x = m + 1, y = m - 1$ là nghiệm của phương trình

k lẻ $\Rightarrow k = 2n + 1 \Rightarrow x = n + 1, y = n$

là nghiệm của phương trình.

3.48 – Khi chia n^3 cho 9, số dư là 0, 1 hay 8. Suy ra phương trình không có nghiệm nguyên khi và chỉ khi $k = 9t \pm 4$

3.49 $(2m^2 + 1)^2 - (m^2 + 1)(2m)^2 = 1$ nên phương trình có nghiệm là $x = 2m^2 + 1, y = 2m$

Từ $(x^2 + Dy^2)^2 - D(2x\, y)^2 = (x^2 - Dy^2)^2$

Suy ra : nếu $(x_0; y_0)$ là nghiệm thì $(x_0^2 - Dy_0^2 ; 2x_0 y_0)$ cũng là nghiệm.

3.50 – $(3x_0 + 2y_0 + 1)^2 + (3x_0 + 2y_0 + 2)^2 = (4x_0 + 3y_0 + 2)^2$; ở vế phải thay $9y_0^2 = 8y_0^2 + y_0^2 = 8y_0^2 + 2x_0^2 + 2x_0 + 1$

$3^2 + 4^2 = 5^2$ $(x_0 = 3, y_0 = 5) \Rightarrow x_1 = 3.3 + 2.5 + 1 = 20.$

$y_1 = 4.3 + 3.5 + 2 = 29 (20^2 + 21^2 = 29^2)$, $x_2 = 119$, $y^2 = 169$

$(119^2 + 120^2 = 169^2)$, v.v...

3.51 – Dễ thấy (1; 1) là nghiệm → (8; 6) → (49; 35) → ...

3.52 – (1; 1) → (22; 13) → (313 ; 181) → (4366; 2521)

3.53 – (3; 2) ⇒ (17; 12) → (99; 70) → (577; 408)

3.54 Không mất tính tổng quát, có thể giả thiết $x \leq y \leq z \leq t$

$$x > 1 \text{ vì } \frac{1}{1} + \frac{1}{y^2} + \frac{1}{z^2} + \frac{1}{t^2} > 1$$

$$t < 3 \text{ vì } \frac{1}{x^2} + \frac{1}{y^2} + \frac{1}{z^2} + \frac{1}{9} < 1$$

Nghiệm duy nhất: $x = y = z = t = 2$

3.55 – a) Có thể giả thiết $0 < x \leq y \leq z$. Rõ ràng là $x > 1$. Mặt khác $x < 4$ vì nếu $x \geq 4$ thì

$$\frac{1}{x} + \frac{1}{y} + \frac{1}{z} \leq \frac{1}{4} + \frac{1}{4} + \frac{1}{4} = \frac{3}{4}$$

Vậy chỉ có thể $x = 2$ hoặc $x = 3$

$$x = 2 \Rightarrow \frac{1}{y} + \frac{1}{z} = \frac{1}{2} \Leftrightarrow (y - 2)(z - 2) = 4 \Leftrightarrow y = 4, z = 4$$

hoặc $y = 3$, $z = 6$

$$x = 3 \Rightarrow \frac{1}{y} + \frac{1}{z} = \frac{2}{3} \Leftrightarrow (2y - 3)(2z - 3) = 9 \Leftrightarrow y = 3.\ z = 3.$$

b) Tương tự 3.54 và 3.55 a)

Có thể giả thiết $0 < x \leq y \leq z \leq t$. Để thỏa mãn phương trình phải có $x > 1$ và $x < 5$, tức $x = 2, 3, 4$

$$x = 2 \Rightarrow \frac{1}{y} + \frac{1}{z} + \frac{1}{t} = \frac{1}{2} \Rightarrow 2 < y < 7\ (y \leq z < t)$$

$$y = 3 \Rightarrow \frac{1}{y} + \frac{1}{z} = \frac{1}{6} \Rightarrow 6 < z < 13,\ z = 7, 8, 9, 10, 11, 12.$$

→ Có 5 nghiệm (với $z = 11$ thì không có giá trị t nguyên)

Tiếp tục với $y = 4$ (có 3 nghiệm), $y = 5$ (có một nghiệm), $y = 6$ (có 1 nghiệm)

$x = 3 \Rightarrow y = 3, 4$. Với $y = 3$, có 2 nghiệm; với $y = 4$ có 1 nghiệm

$x = 4$, có 1 nghiệm.

3.56 – Với mọi bộ ba số $(x; y; z)$ thỏa mãn phương trình, giả sử $0 < x \le y \le z$ thì

$$0 < \frac{1}{z} \le \frac{1}{y} \le \frac{1}{x} \Rightarrow \frac{1}{x} < \frac{1}{x} + \frac{1}{y} + \frac{1}{z} = \frac{1}{1991} \le \frac{3}{x}$$

$\Rightarrow 1991 < x \le 3.1991$, nghĩa là x lấy một số hữu hạn giá trị (không nhiều hơn 2.1991). Với mỗi giá trị của x, có

$$\frac{1}{1991} - \frac{1}{x} = \frac{1}{y} + \frac{1}{z} \le \frac{2}{y} \Rightarrow y \le \frac{2.1991x}{x - 1991} \le 2^2.1991$$

Với x, y đã biết thì có nhiều nhất là một giá trị tương ứng của

Vậy có tất cả không quá $2^3.1991$ nghiệm.

Có thể thấy ngay một nghiệm là $x = y = z = 3.1991$

3.57 – a) Xét $\frac{1}{x} + \frac{1}{y} = \frac{1}{a}$ (a nguyên dương)

$$\Leftrightarrow ax + ay = xy \quad \Leftrightarrow \quad (x - a)(y - a) = a^2$$

Có tất cả $2r - 1$ nghiệm, với r là số các ước số của a^2:

$$\begin{cases} x - a = d \\ y - a = a^2/d \end{cases} \quad \begin{cases} x - a = -d \\ y - a = -a^2/d \end{cases}$$ d là một ước số của a.

(trừ $x - a = -a$, $y - a = -a \Rightarrow x = 0$, $y = 0$, vô nghĩa)

Với $a = 14$, $a^2 = 1996$ có các ước là (9 ước)

1, 2, 4, 7, 14, 28, 49, 98, 196

và phương trình có $2.9 - 1 = 17$ nghiệm. Thí dụ với $d = 4$

có $\begin{cases} x - 14 = 4 \\ y - 14 = 49 \end{cases}$ tức $\begin{cases} x = 18 \\ y = 36 \end{cases}$ và $\begin{cases} x - 14 = -4 \\ y - 14 = -49 \end{cases}$ tức $\begin{cases} x = 10 \\ y = -35 \end{cases}$

b) Có phương trình tương đương :

$$(x - z)(y - z) = z^2$$

Gọi $t = (x, y, z)$, tức $x = x_1 t$, $y = y_1 t$, $z = z_1 t$, $(x_1, y_1, z_1) = 1$

$m = (x_1, z_1)$ tức $x_1 = mx_2$; $z_1 = mz_2$, $(x_2, z_2) = 1$

$n = (y_1, z_1)$ tức $y_1 = ny_2$, $z_1 = nz_3$, $(y_2, z_3) = 1$

$\Rightarrow (m, n) = 1$ vì $(x_1, y_1, z_1) = 1$

và $z_1 = mnp$ vì $z_1 = mz_2 = nz_3$

thay $x = mx_2t$, $y = ny_2t$, $z = mnpt$ vào (1) và rút gọn cho mnt^2 được

$$(x^2 - np)(y^2 - mp) = mnp^2 \quad (2)$$

$$x_2y_2 = (x_2^m + y_2^n)p$$

$\Rightarrow x_2y_2 \vdots p$ mà $(x_2, p) = 1$ do $m = (x_1, z_1) = (mx_2, mnp)$,

$(y_2, p) = 1$ do $n = (y_1, z_1) = (ny_2, mnp)$

$\Rightarrow p = 1$ và (2) thành

$(x_2 - n)(y_2 - m) = mn$

$(x_2, n) = 1$ vì $(x_1, y_1, z_1) = (mx_2, ny_2, mn) = 1$

$\Rightarrow (x_2 - n, n) = 1 \Rightarrow y_2 - m \vdots n$

Tương tự : $x_2 - n \vdots m$

$$\Rightarrow x_2 - m = \pm n,\ y_2 - n = \pm m$$

Tức $\quad x_2 = m \pm n, \quad y_2 = n \pm m$

Công thức của nghiệm tổng quát là:

$x = m(m \pm n)t$, $y = n(n \pm m)t$, $z = mnt$

3.58 – Thử trực tiếp với $x < 5$, có nghiệm à $x = 1$, $y = \pm 1$ và $x = 3$, $y = \pm 3$. Còn với $x \geq 5$, phương trình vô nghiệm:

$1! + 2! + 3! + 4! = 33$, còn $5!, 6!, 7! \ldots$ đều tận cùng là 0, vì vậy $1! + 2! + \ldots + x!$ tận cùng bằng 3 với $x \geq 5$, trong khi đó y^2 không thể tận cùng là 3.

4.3 $\quad \overline{xyzt} - 2.\overline{yzt} = 1000x - \overline{yzt} = \overline{xz}$

$\Rightarrow 990x = 100y + 11z + t$, trong đó $0 \leq y,z,t \leq 9$, $0 < x \leq 9$

$\Rightarrow x = 1 \Rightarrow 990 = 100y + 11z + t \Rightarrow y = 9.$

$\Rightarrow 90 = 11z + t \Rightarrow z = 8.$ Đáp số 1982.

4.4 $100x + 10y + z < 10(x + 1)$ (chú ý: $0 \le y,z \le 9$, $0 < x \le 9$)

Nếu y hoặc z khác 0 thì $x + y + z \ge x + 1$

$$\Rightarrow t = \frac{100x + 10y + z}{x + y + z} \le \frac{100(x + 1)}{x + 1} = 100$$

$y = z = 0 \Rightarrow t = 100$

4.5 $a_n \dots a_1 a_0 7$ $\quad 5 \times 7 = 35 \quad \Rightarrow a_0 = 5$ (nhớ 3)

$\times 5 \quad 5a_0 + 3 = 28 \quad \Rightarrow a_1 = 8$ (nhớ 2)

$7a_n \dots a_2 a_1 a_0 \quad 5a_1 + 2 = 24 \quad \Rightarrow a_2 = 2$ (nhớ 4)

...

Cho đến $a_5 = 7$ thì kết thúc.

Số 714285.

4.6 – $a = 1, 4, 9 \Rightarrow \overline{ad} = 16, 49$ (không có $\overline{9d}$ là chính phương)

$\Rightarrow d = 6, 9 \Rightarrow \overline{cd} = 16, 36, 49 \Rightarrow \overline{abcd} = 1936$

4.7 – $a + b \ge 7$ (1), $a^2 + b^2 \le 30$ (2) $10a + b > 2(10b + a)$ (3)

(1) và (2) $\Rightarrow a = 2$, $b = 5$ hoặc $a = 5$, $b = 2$

(3) $\Rightarrow 8a > 19b$ Vậy $a = 5$, $b = 2$. Đáp số 52.

4.8 – $10x + y = kxy$ có nghiệm với $k = 1, 2, 5 \Rightarrow 11, 12, 15, 24, 36.$

4.9– $P = \overline{abcdez} = \overline{abc}.1000 + \overline{dez}$, $P + (\overline{abc} - \overline{dez}) = \overline{abc}.1001$

4.10 $P = \overline{abc}$, $a + b + c = 7k \Rightarrow a = 7k - b - c$

$\Rightarrow P = 100(7k - b - c) + 10b + c = 100.7k - 90b - 99c$

$= 100.7k - 13.7b + b - 14.7c - c = 7.M + (b - c)$

4.11 $M = \overline{a_n \dots a_1 a_0}$, $N = \overline{a_n \dots a_1} + 4a_0$

$10N - M = \overline{a_n \dots a_1}.10 + 40a_0 - \overline{a_n \dots a_1}.10 - a_0 = 39 a_0 \vdots 13$

vì $(10, 13) = 1$ nên $10N \vdots 13 \Leftrightarrow N \vdots 13$

4.12– $M = \overline{a_n \dots a_1 a_0}$, $N = 3.\overline{a_n \dots a_1} + 2a_0 \Rightarrow 2M - N \vdots 17$

4.13 $(8, 9) = 1 \Rightarrow N = \overline{1234xy} = 123400 + \overline{xy} = 72.1713 + 64 + \overline{xy}$

$$N \vdots 8.9 = 72 \Leftrightarrow 64 + \overline{xy} \vdots 72$$

$\Rightarrow 64 + \overline{xy} = 72 \Rightarrow \overline{xy} = 08$ hoặc $64 + \overline{xy} = 144 \Rightarrow \overline{xy} = 80$

4.14 $\overline{abc} - (a + b + c) = 99a + 9b = 9(11a + b) \vdots 9$. Tổng các chữ số của hiệu này chia hết cho 9, vì vậy nếu tiếp tục thì mỗi lần giảm đi 18 hoặc 9 và cuối cùng phải đến 0.

4.16 – a) 2111_3 b) 11011_2 c) 700034_9

d) kí hiệu A = 10, B = 11 thì có $B0AA_{13}$

4.17 a) cơ số 6; 7; 5 ≥ 8

b) 7_8 ; 22_3; 111_2; 4444_5

4.18 a) $2x + 3 = 3y + 2 \Rightarrow x = 4, y = 3$ hoặc $x = 7, y = 5$

4.19 a) $2_3 + 1_3 = 10_3$, $3_4 + 2_4 = 11_4$, $45_6 + 51_6 = 140_6$

b) 5 + 4 cho 2, thức 5 + 4 = 12, cơ số 7.

4.20 Số theo cơ số 6.

4.21 a) $121_g = g^2 + 2g + 1 = (g + 1)^2$

c) $g^3 + 3g^2 + 3g + 1 = (g + 1)^3$

4.22 – a) $N = (a_n \dots a_1a_0)_g = M.g + a_0$. Nếu d là ước của g thì

$$N \vdots d \Leftrightarrow a_0 \vdots d.$$

Trong hệ cơ số 12 chẳng hạn thì dấu hiệu chia hết cho 2, 3, 4, 6 (các ước của 12) là chữ số tận cùng chia hết cho số tương ứng.

b) $(a_n \dots a_1 a_0)_g \vdots g - 1 \Leftrightarrow a_n + \dots + a_1 + a_0 \vdots g - 1$

$(a_n \dots a_1a_0)_g \vdots g + 1 \Leftrightarrow a_0 - a_1 + a_2 - a_3 + \dots \vdots g + 1$

Chứng minh tương tự chứng minh dấu hiệu chia hết cho 9, cho 11 trong hệ thập phân.

4.23 – a) $N = (a_n \dots a_0)_g$ $S = a_n + \dots + a_0$, $N - S = m.d$

$N = g = (10)_g \Rightarrow S = 1 + 0 = 1 \Rightarrow g = 1 + md$

$$\Rightarrow d = \frac{g - 1}{m}$$

b) $d = 3 \Rightarrow g = 4, 7, 10, 13\dots$ (m = 1, 2, 3, 4...)

$d = 9 \Rightarrow g = 10, 19, 28\dots$ (m = 1, 2, 3 ...)

$\Rightarrow g = 10, 19, 28... (m = 1, 2, 3 ...)$

4.24 $(10101)_g = g^4 + g^2 + 1 = \dfrac{g^6 - 1}{g^2 - 1} = (g^2 + g + 1)(g^2 - g + 1)$

$$(1010101)_g = g^6 + g^4 + g^2 + 1 = \frac{g^8 - 1}{g^2 - 1} = (g^2 + 1)(g^4 + 1)$$

4.25 $2.\overline{abc} = (abc)_g \Rightarrow P = (200 - g^2)a + (20 - g)b + c = 0$

Trong đó $1 \le a \le 9$, $0 \le b,c \le 9$, $g > a$, $g > b$, $g > c$.

Cơ số g không thể ≤ 14 hoặc ≥ 16

($g \le 14 \Rightarrow P \ge 4$; $g \ge 16 \Rightarrow$ => $P \le -11$)

$g = 15 \Rightarrow P = -25a + 5b + c = 0 \Rightarrow c = 0$ hoặc $c = 5$.

$c = 0 \Rightarrow a = 1, b = 5,$ $\overline{abc} = 150$

$c = 5 \Rightarrow a = 1, b = 4,$ $\overline{abc} = 145$

$a = 2$, $b = 9,$ $\overline{abc} = 295$

4.36 a) Không.

b) Không quá 10 câu, vì số từ 0 đến 1000 chuyển sang hệ nhị phân thì có không quá 10 chữ số.

4.37 – Viết a, b, c trong hệ nhị phân:

$a = (a_2\ a_1\ a_0)_2$ $3 = (0\ 1\ 1)_2$

$b = (b_2\ b_1\ b_0)_2$ $5 = (1\ 0\ 1)_2$

$c = (c_2\ c_1\ c_0)_2$ $7 = (1\ 1\ 1)_2$

Lấy tổng các số biểu diễn bởi các chữ số trong từng hàng:

$a_0 + b_0 + c_0$ $a_1 + b_1 + c_1$ $a_2 + b_2 + c_2$

Các tổng này có thể lẻ (như $a_0 + b_0 + c_0 = 1 + 1 + 1$) hoặc *chẵn* ($a_1 + b_1 + c_1 = 1 + 0 + 1$, $a_2 + b_2 + c_2 = 0 + 1 + 1$)

Người đi trước (A) dùng chiến thuật: lấy một số que ở một đống sao cho sau đó *mọi tổng trên đều là chẵn*. Thí dụ: lấy 1 que ở bất kỳ đống nào (để có $a_0 + b_0 + c_0 = 1 + 1$ trong khi các tổng khác vẫn là chẵn) lấy ở đống thứ ba chẳng hạn. Lúc đó, người đi sau (B) sẽ đứng trước ba đống với số que như sau:

$$3 = (0\ 1\ 1)_2$$
$$5 = (1\ 0\ 1)_2$$
$$6 = (1\ 1\ 0)_2$$

Trong đó mọi tổng $a_0 + b_0 + c_0$, $a_1 + b_1 + c_1$, $a_2 + b_2 + c_2$ đều *chẵn*; B lấy đi bao nhiêu que ở một đống nào cũng làm cho *ít nhất một trong ba tổng trên trở thành số lẻ*. Đến lượt mình, A lại lấy một số que để cho *mọi tổng trên đều chẵn*. Cuối cùng, A làm cho mọi tổng đó đều bằng 0, tức là A thắng.

Chú ý rằng như vậy nếu ban đầu cho ba đống với 3, 5, 6 que thì người đi sau sẽ thắng (nếu biết cách chơi).

Có thể dễ dàng mở rộng trò chơi với nhiều đống, và số que ở mỗi đống là số tùy ý cho trước.

TÀI LIỆU THAM KHẢO

1. H. Davenport, The higher arithmetic (bản dịch tiếng Nga) M, 1965.

2. W. Sierpinski, Những gì chúng ta đã biết và chưa biết về số nguyên tố (bản dịch tiếng Nga), M. 1963

3. Sierpinski, Về giải các phương trình trong tập hợp số nguyên (bảng dịch tiếng Nga), M. 1961

4. W. Sierpinski, 250 bài toán số học (bản dịch tiếng Nga), M. 1968

5. G.Rademakhơ, O. Toeplitz, Số và hình (bản dịch tiếng Nga), M. 1966

6. R. Coourant, H. Robbins, What is Mathematics? (bản dịch tiếng Nga), M. 1966

7. E. B. Đưnkin, V. A. Utspenski, Các bài nói chuyện về toán học, M. 1962 (tiếng Nga)

8. C. V. Fomin, Các hệ ghi số, M. 1968 (tiếng Nga)

9. I. Depman, Chuyện kể về đại số cũ và đại số mới, Leningrad, 1967 (tiếng Nga)

10. A.N.Kolmogorov (chủ biên), Đại số và mở đầu về ải tích, lớp 9, M.1978 (tiếng Nga)

11. A.G. Mordkovich, Algebra and Elements of Mathen al Analysis, Mir Publishers, M. 1989

12. V.N.Caxatkin, Nhập môn điều khiển học (cho h nh lớp 9), Kiev,1986 (tiếng Nga)

13. D.O.Sliarski, N.N.Senxov, I.M.Iaglom, Tuyển tập các bài toán và định lý về toán học sơ cấp - Số học và đại số, M.1965 (tiếng Nga)

14. I.L.Babinskaia, Các bài toán bồi dưỡng và thi học sinh giỏi của Liên Xô, Nguyễn Quí Di... dịch, SGD tp Hồ Chí Minh, 1988

15. X.V. Conhighin,.. Các đề thi vô địch toán của các nước, SGD Hải Phòng, 1990

16. B.V. Gnhiedenko(chủ biên), Từ điển bách khoa của nhà toán học trẻ, M.1985 (tiếng Nga)

17. Iu.V.Prokhorov (chủ biên), Từ điển bách khoa toán học, M. 1988 (tiếng Nga)

18. Lại Đức Thịnh, Số học lớp 6, tập I, NXB GD, 1984

19. Nguyễn Hữu Hoan, Số học phổ thông, NXB Đại học THCN, 1986

20. Vũ Dương Thụy, Trương Công Thành, Nguyễn Ngọc Đạm, 400 bài toán số học chọn lọc, SGD Hà Sơn Bình, 1986

21. Đinh Gia Phong, Nguyễn Hữu Thảo, Các bài thi chọn học sinh giỏi toán cấp II (từ 1964 đến 1985), NXB GD, 1987

22. Hoàng Chúng, Thử suy nghĩ khác một chút về mấy khái niệm và bài toán quen thuộc, Trung Tâm BDGV, tp Hồ Chí Minh, 1990

23. Hoàng Chúng, Đôi điều cần thiết về logic, Trung Tâm BDGV, tp Hồ Chí Minh, 1990

24. Báo Toán học và tuổi trẻ

MỤC LỤC

*

Chịu trách nhiệm xuất bản

Giám đốc: PHẠM VĂN AN

Tổng biên tập: NGUYỄN NHƯ Ý

Biên soạn

HOÀNG CHÚNG

Trình bày bìa

ĐỖ DUY NGỌC

In 3000 cuốn tại Xưởng in Cty ĐTPTVH.
Giấy phép xuất bản số 214 / CXB- 849 do Cục Xuất bản cấp ngày 22 tháng 3 năm 1997.
In xong và nộp lưu chiểu tháng 6 năm 1997.

Giá : 9.000đ